Minimum number of input states required for quantum gate characterization

Daniel M. Reich, Giulia Gualdi,* and Christiane P. Koch†
Theoretische Physik, Universität Kassel, Heinrich-Plett-Str. 40, D-34132 Kassel, Germany
(Received 8 August 2012; published 8 October 2013)

We derive an algebraic framework which identifies the minimal information required to assess how well a quantum device implements a desired quantum operation. Our approach is based on characterizing only the unitary part of an open system's evolution. We show that a reduced set of input states is sufficient to estimate the average fidelity of a quantum gate, avoiding a sampling over the full Liouville space. Surprisingly, the minimal set consists of only two input states, independent of the Hilbert-space dimension. The minimal set is, however, impractical for device characterization, since one of the states is a totally mixed thermal state and extracting bounds for the average fidelity is impossible. We therefore present two further reduced sets of input states that allow for, respectively, numerical and analytical bounds on the average fidelity.

DOI: 10.1103/PhysRevA.88.042309 PACS number(s): 03.67.Ac, 03.65.Ta, 03.65.Wj, 03.67.Pp

I. INTRODUCTION

The usual measure to assess how well a quantum device implements a desired quantum operation is the average fidelity:

$$F_{\text{av}} = \int \langle\Psi|O^{+}\mathcal{D}(|\Psi\rangle\langle\Psi|)O|\Psi\rangle d\Psi, \qquad (1)$$

where O denotes the desired unitary and the actual time evolution is described by the dynamical map $\mathcal{D}$. The standard approach to determine F_{av} relies on quantum process tomography [1]. In practice, the average fidelity of a quantum process in a d-dimensional Hilbert space is often estimated by performing quantum state tomography in a d^2-dimensional Hilbert space. For N qubits, $d = 2^N$. The fidelity can also be obtained by determining the process matrix, which is of size $d^2 \times d^2$. In both cases quantum process tomography scales exponentially in resources [2]. For quantum devices to be realized and tested in practical applications, a less resource-intensive approach to characterization is required.

Recent attempts at reducing the required resources employ stochastic sampling of the input states and measurement observables [3–6]. The process matrix can be estimated efficiently if it is sparse in a known basis [5–7]. For general unitary operations and without assuming any prior knowledge, Monte Carlo sampling to determine state fidelities in the d^2-dimensional Hilbert space currently seems to be the most efficient approach [3,4,8]. This is due to the fact that the approach directly targets the fidelity between the desired operation and the implemented process rather than fully characterizing the process and subsequently comparing it to the desired operation. It also comes with the advantage of separable input states and Pauli measurements. For N qubits, this approach requires the ability to prepare 6^N input states, since there are six eigenstates for the three Pauli operators for each qubit, and the ability to measure all of the $d^2 = 2^{2N}$ operators that form an orthonormal Hermitian operator basis.

Another approach to the estimation of the average fidelity exploits its property of being a second-degree polynomial in the states, utilizing a so-called two design [9]. A commonly used two design is made up of the $d(d+1)$ states of $d+1$ mutually unbiased bases. The average fidelity is then written as a sum over state fidelities for these states [9]. The latter implies preparation of entangled input states, since only three out of the $d+1$ mutually unbiased bases consist of separable states [10]. Both Monte Carlo characterization and the two-design approach yield the average fidelity with an arbitrary prespecified accuracy. Alternatively, bounds on the average fidelity can be obtained from two classical fidelities [11] where each classical fidelity is expressed as a sum over d state fidelities. The different requirements of Monte Carlo characterization, the two-design approach and the two classical fidelities in terms of the number of input states, raise the question of what is the minimal set of states to determine F_{av}.

Here we show that a minimal set of states can be identified by the requirements to allow for distinguishing any two unitaries and assess whether the time evolution is unitary. We find the minimal set of states to consist of only two states, independent of the size of Hilbert space. The minimal set contains, however, a totally mixed thermal state which is impractical for experiments. We therefore also introduce a reduced set of states that consists of the minimum number of pure states required to distinguish any two unitaries and assess whether the time evolution is unitary. The average fidelity can then be estimated by evaluating a distance measure for the reduced set of states. The corresponding protocol consists of preparing $d+1$ pure states, defined in d-dimensional Hilbert space, and measuring the corresponding state fidelities. We show numerically that the estimate of the gate error differs from F_{av} by a factor of less than 2.5 in the worst case and 1.2 on average. We furthermore demonstrate that evaluation of state fidelities for the reduced set of states is also sufficient to quantify the nonunitarity of the process. This allows us to determine whether the gate error is due to decoherence or due to unitary errors that are easier to mitigate.

If analytical instead of numerical bounds on the average fidelity are desired, the reduced set needs to contain $2d$ states; i.e., our approach generalizes the estimate of the average fidelity in terms of two classical fidelities [11]. We show

*Present address: QSTAR, Largo Enrico Fermi 2, I-50125 Florence, Italy.
†christiane.koch@uni-kassel.de

that the specific states utilized by Refs. [11,12] also fulfill the requirements for distinguishing any two unitaries and assessing unitarity of the time evolution—as do the states of any two mutually unbiased bases.

Our paper is organized as follows: The algebraic framework for identifying the minimum requirements to distinguish any two unitaries and assess unitarity of the time evolution is derived in Sec. II, introducing the concepts of commutant space and total rotation. Section III presents the reduced sets of states and discusses their use for extracting an estimate of the average fidelity. The relationship of our approach to the two classical fidelities of Ref. [11] is established in Sec. IV, and our results are summarized in Sec. V. Detailed proofs of the claims made in Sec. II are provided in the Appendix.

II. ALGEBRAIC FRAMEWORK: COMMUTANT SPACE AND TOTAL ROTATION

To identify the reduced set of states, we introduce the concepts of commutant space of a set of density operators and total rotation. We assume purely coherent time evolution with an unknown unitary $U \in U(d)$, such that $\rho(T) = \mathcal{D}(\rho) = U\rho U^+$, and generalize later to nonunitary time evolution. Since the evolution is insensitive to a global phase, U is an element of the projective unitary group, $PU(d)$, i.e., the quotient $U(d)/U(1)$ of the unitary groups $U(d)$ and $U(1)$. Given a set of states, $\{\rho_j = \rho_j(t=0)\}$, we consider the map $\mathcal{M} : PU(d) \longrightarrow \bigoplus_j \mathbb{C}^{d\times d}$, mapping the unitary U onto the set of time-evolved states, $\{\rho_j^U(T) = U\rho_j U^+\}$. We can differentiate any two unitaries U, U' if and only if the map $\mathcal{M}$ is injective. We show that $\mathcal{M}$ is injective if the commutant space of the set $\{\rho_j\}$ has only one element, the identity.

We define the commutant space $K(\rho)$ of a single density operator ρ as the set of all linear operators in $PU(d)$ that commute with ρ. It contains the identity and all operators that have a common eigenbasis with ρ. Unitaries $\tilde{U}$ in the commutant space of ρ cannot be distinguished from $\mathbb{1}$ by time-evolving ρ since $\tilde{U}\rho\tilde{U}^+ = \tilde{U}\tilde{U}^+\rho = \rho$. Therefore, to distinguish a unitary U from the identity, the time evolution of at least two density operators with different eigenbases is required. Once we can differentiate an arbitrary unitary from the identity, we can differentiate it from any other unitary (and $\mathcal{M}$ is injective). This follows from the fact that $PU(d)$ is a group. We define the commutant space of a set of density operators, $\mathcal{K}(\{\rho_j\})$, as the intersection of all $K(\rho_j)$, i.e., the set of all linear operators that commute with *each* ρ_j. Suppose the identity is the only element of the commutant space $\mathcal{K}(\{\rho_j\})$. Then the identity is the only time evolution that leaves *all* ρ_j unchanged and we can distinguish the identity from all other time evolutions by inspecting the time-evolved states. The detailed proof that injectivity of $\mathcal{M}$ is equivalent to $\mathcal{K}(\{\rho_j\})$ having identity as its only element is given in the Appendix.

In order to determine the states of the reduced set $\{\rho_j\}$ that have a commutant space $\mathcal{K}(\{\rho_j\})$ with identity as its only element, we introduce the concept of total rotation. Unitary evolution corresponds to rotations in Hilbert space. Spanning the Hilbert space by an arbitrary complete orthonormal basis $\{|\varphi_i\rangle\}$, a complete set of d one-dimensional orthonormal projectors is obtained, $\mathcal{P}_c \equiv \{P_i = |\varphi_i\rangle\langle\varphi_i|\}$. We construct density operators within this basis, for example, by choosing a single state, $\rho_B = \sum_{i=1}^d \lambda_i P_i$ with $\lambda_i \neq \lambda_j$ for $i \neq j$, or a set of d states, $\{\rho_{B,i}\}$, $\rho_{B,i} = P_i$, $i = 1,\ldots,d$. The time-evolved basis state $\rho_B(T)$ or states $\{\rho_{B,i}(T)\}$ allow for distinguishing all those unitaries from identity that do not have common eigenspaces with all P_i. To distinguish the remaining unitaries from identity, we construct one additional state, ρ_{TR}, that is guaranteed to have no common eigenspace with any P_i. This is achieved by introducing a totally rotated one-dimensional projector P_{TR} obeying $P_{\mathrm{TR}} P_i \neq 0\ \forall P_i \in \mathcal{P}_c$ and taking $\rho_{\mathrm{TR}} = P_{\mathrm{TR}}$. Adding P_{TR} to $\mathcal{P}_c$ makes the set of projectors complete and totally rotating, $\mathcal{P}_{cTR} = \mathcal{P}_c \cup \{P_{\mathrm{TR}}\}$. A set of states $\{\rho_j\}$ is complete and totally rotating if the subset of the projectors onto the one-dimensional eigenspaces of the $\{\rho_j\}$ is complete and totally rotating. For example, $\{\rho_B,\rho_{\mathrm{TR}}\}$ or $\{\rho_{B,1},\ldots,\rho_{B,d},\rho_{\mathrm{TR}}\}$. We show in the Appendix that the identity is the only projective unitary operator that has a common eigenbasis with all elements of such a set of states.

We have thus constructed a reduced set of states $\{\rho_j\}$ that allows for differentiating any two unitaries by inspection of the time-evolved states, $\{\rho_j(T)\}$. For coherent time evolution, we can evaluate

$$F_j = \mathrm{Tr}\big[\rho_j^O \rho_j(T)\big], \tag{2}$$

which matches each state ρ_j, subjected to the ideal operation, $\rho_j^O = O\rho_j O^+$, to the actually evolved state, $\rho_j(T) = \mathcal{D}(\rho_j)$, for all $\rho_j(T)$. A suitable combination of the resulting F_j yields an estimate of F_{av}. However, for a possibly incoherent time evolution, we need to quantify the "nonunitarity" of the actual evolutions $\mathcal{D}(\rho_j)$. This can be done by checking whether $\mathcal{D}$ maps projectors onto projectors, reflecting rotations in Hilbert space. We show in the Appendix that indeed unitarity of a dynamical map $\mathcal{D}$ is equivalent to $\mathcal{D}$ mapping (i) a set $\{P_i\}$ of d one-dimensional orthogonal projectors onto another such set $\{\tilde{P}_i\}$ of d one-dimensional orthogonal projectors and (ii) a projector P_{TR} that is totally rotated with respect to the set $\{P_i\}$ onto a one-dimensional projector.

III. REDUCED SET OF STATES YIELDING NUMERICAL BOUNDS ON THE AVERAGE FIDELITY

A set of density operators that allows for both differentiating any two unitaries and measuring the nonunitarity of any dynamical map $\mathcal{D}$ is thus given by

$$\rho_{B,i} = |\varphi_i\rangle\langle\varphi_i|, \quad i = 1,\ldots,d, \tag{3a}$$

$$\rho_{\mathrm{TR}} = \frac{1}{d}\sum_{i,j=1}^{d} |\varphi_i\rangle\langle\varphi_j|. \tag{3b}$$

By construction, the states $\rho_{B,i}$, ρ_{TR} are pure. They are separable if a separable basis is chosen, i.e., if all $|\varphi_i\rangle$ are separable. Another suitable reduced set to differentiate any two unitaries and measure nonunitarity of $\mathcal{D}$ is given by

$$\left\{\rho_B = \sum_i \lambda_i P_i, \rho_{\mathrm{TR}}\right\} \quad \text{with} \quad \lambda_i \neq \lambda_j \quad \text{for} \quad i \neq j. \tag{4}$$

This is the minimal set.[1] However, for the characterization of quantum gates, it is preferable to use the pure input states defined in Eq. (3). Each of these states, when evolved in time, is characterized, to leading order, by d^2 real parameters. Knowledge of the total $d^2(d+1)$ parameters is sufficient to determine whether the time evolution matches the desired unitary.

Note that both reduced sets are also sufficient to reconstruct a unitary that is close to a given open system evolution. This implies that, in optimal control calculations for quantum gates in the presence of decoherence, propagation of two states, $\{\rho_B = \sum_i \lambda_i P_i, \rho_{\rm TR}\}$ independent of the system size d, is sufficient. This reduces significantly the numerical effort compared to the d^2 states used to date [13].

A. Estimating the gate error

The usual figure of merit in quantum process tomography, the average fidelity $F_{\rm av}$ or, respectively, the gate error $1 - F_{\rm av}$, can be estimated by averaging over the distance measures F_j, Eq. (2), for each state ρ_j in the reduced set. Each F_j becomes maximal if and only if $O\rho_j O^+ = \mathcal{D}\rho_j$. Our protocol thus consists in the preparation of $d+1$ states ρ_j, Eq. (3), and measurement of the corresponding state fidelities, F_j, for the time-evolved states, $\mathcal{D}(\rho_j)$. A possible choice of states is, e.g.,

$$\left(\rho^O_{B,i}\right)_{nm} \equiv (P_i)_{nm} = \delta_{ni}\delta_{mi} \tag{5}$$

in the computational basis. The average over the F_j can employ the arithmetic mean or a modified geometric mean,

$$F^{\rm arith}_{\rm unitary} = \frac{1}{d+1}\left[\sum_{i=1}^{d} F_{B,i} + F_{\rm TR}\right], \tag{6}$$

$$F^{\rm geom}_{\rm unitary} = \frac{1}{d+1} + \left(1 - \frac{1}{d+1}\right)\left[\prod_{i=1}^{d} F_{B,i} \cdot F_{\rm TR}\right], \tag{7}$$

or a combination of the two. The first term in Eq. (7) ensures $F^{\rm geom}_{\rm unitary}$ to take values in the same interval, $[\frac{1}{d+1}, 1]$, as $F_{\rm av}$ for unitary evolution. $F^{\rm arith/geom}_{\rm unitary} = 1$ only for a purely coherent time evolution that perfectly implements the desired gate O for all states in the reduced set. While the arithmetic mean weights all state fidelities linearly, the geometric mean works best if the error is due to a single F_j. An optimized way to extract information from all the F_j is obtained by a suitable combination of the arithmetic and geometric mean: We define a fidelity that switches from the arithmetic mean to the geometric one, should the state fidelities for all the $\rho_{B,i}$ be close to 1:

$$F^{\lambda}_{\rm unitary} = \lambda F^{\rm geom}_{\rm unitary} + (1-\lambda) F^{\rm arith}_{\rm unitary}, \tag{8a}$$

with

$$\lambda = 1 - \frac{1 - \prod_{i=1}^{d} F_{B,i}}{1 - \prod_{i=1}^{d} F_{B,i} \cdot F_{\rm TR}}. \tag{8b}$$

[1]The corresponding extension of the proof requires $\mathcal{D}$ to be unital. Any distance measure based on $\{\rho_B = \sum_i \lambda_i P_i, \rho_{\rm TR}\}$ must therefore contain an additional check whether $\mathcal{D}$ maps the identity onto itself. which can be performed by adding a suitable third state to the set.

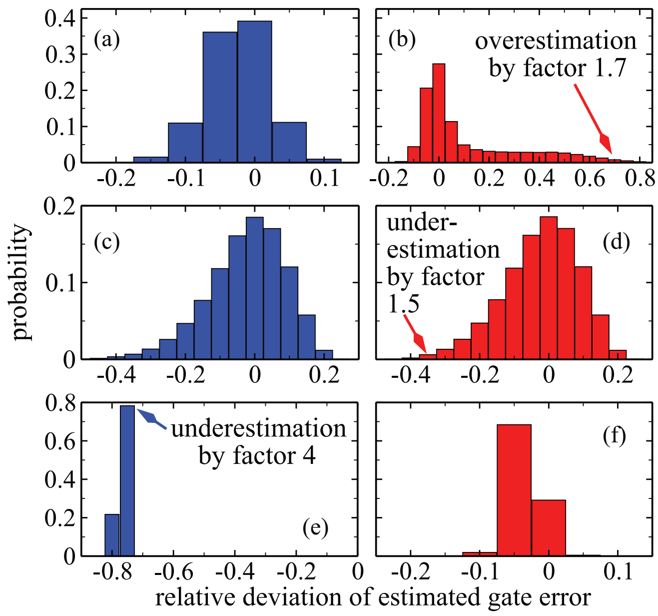

FIG. 1. (Color online) Probability of the estimated gate error's relative deviation from the standard gate error, $\Delta = (\varepsilon_{\rm estim} - \varepsilon_{\rm av})/\varepsilon_{\rm av}$, for 100.000 realizations when using $F^{\rm arith}_{\rm unitary}$, Eq. (6) (left column), and $F^{\lambda}_{\rm unitary}$, Eq. (8) (right column). Shown are the results for (a, b) randomized dynamical maps with $O =$ CNOT, (c, d) truly random unitaries with $O =$ CNOT, and (e, f) randomized unitaries with $O = \mathbb{1}$. Positive and negative values of Δ, corresponding to under- and overestimation of the gate error, do not scale equivalently. The scale for overestimation ($\Delta > 0$) ranges from zero to infinity while that for underestimation ($\Delta < 0$) is confined to $[-1,0)$.

The choice of λ is motivated as follows: $\lambda = 1$ such that $F^{\lambda}_{\rm unitary} = F^{\rm geom}_{\rm unitary}$ if $F_{B,i} = 1$ for all i, i.e., in cases where the gate error is captured by $F_{\rm TR}$ alone; and $\lambda = 0$ yielding $F^{\lambda}_{\rm unitary} = F^{\rm arith}_{\rm unitary}$ if $F_{\rm TR} = 1$, i.e., when the gate error is comprised in the $F_{B,i}$.

Figure 1(a) shows the probability of obtaining a certain relative deviation of the estimated gate error for randomized dynamical maps and CNOT as the target gate. The randomized dynamical maps were obtained by creating a random matrix [14] for twice as many qubits as there are system qubits. The random matrices were hermitized, multiplied by a randomly chosen scaling factor, and exponentiated. The resulting matrix was multiplied by the tensor product of the target unitary with $\mathbb{1}$, and the bath qubits were traced out. For most dynamical maps, $F^{\rm arith}_{\rm unitary}$ yields a good estimate of the gate error. If, however, the state fidelities for all $\rho_{B,i}$ are very high, but the fidelity for the totally rotated state is comparatively small, the arithmetic mean seriously underestimates the gate error. This can happen, for example, if the evolution is perfectly unitary, $\mathcal{D}(\rho_j) = \tilde{U}\rho_j\tilde{U}^+$, and $\tilde{U}$ and the target O have a common eigenbasis with all the $\rho_{B,i}$. Then the information relevant for the gate error is completely contained in $F_{\rm TR}$. This is illustrated in Fig. 1(e) for randomized unitaries with an eigenbasis very close to the $\rho_{B,i}$ and $O = \mathbb{1}$. In such a case the geometric average over all state fidelities will yield a much better estimate of the gate fidelity. In most cases, however, the geometric mean is too strict and overestimates the gate error, motivating the definition Eq. (3). Indeed, the best estimates

TABLE I. Numerically obtained bounds for over- and underestimation of the average fidelity of the form $\alpha^i F^i_{\text{unitary}} \leqslant F_{\text{av}} \leqslant \beta^i F^i_{\text{unitary}}$ for the arithmetic mean over the state fidelities (i = arith) and the combination of arithmetic and geometric mean ($i = \lambda$), using 100.000 realizations, for two and three qubits with O corresponding to CNOT ($N = 2$), the Toffoli gate ($N = 3$), and identity (randomized unitaries).

N	Type of dynamics	α^{arith}	β^{arith}	α^{λ}	β^{λ}
2	Randomized dynamical map	0.83	1.31	0.44	1.26
	Random unitaries	0.76	2.35	0.75	1.92
	Randomized unitaries	1.00	4.39	0.90	1.15
3	Randomized dynamical map	0.96	1.04	0.51	1.03
	Random unitaries	0.90	1.32	0.90	1.32
	Randomized unitaries	1.00	8.67	0.91	1.20

of the gate error are obtained using $\varepsilon^{\lambda}_{\text{unitary}} = 1 - F^{\lambda}_{\text{unitary}}$ as shown in the right part of Fig. 1. Figures 1(a), 1(b), 1(e), and 1(f) present results for randomized dynamical maps and randomized unitaries that were generated by exponentiating random Hermitian matrices. Since this is not truly random, we have also generated random unitaries based on Gram-Schmidt orthonormalization of randomly generated complex matrices [15] [cf. Figs. 1(c) and 1(d) with O = CNOT]. $\varepsilon^{\lambda}_{\text{unitary}}$ yields a faithful estimate of the gate error in all cases. On average, it underestimates the gate error by factors 1.03 [Fig. 1(b)], 1.11 [Fig. 1(d)], and 1.02 [Fig. 1(f)] and overestimates it by 1.16 [Fig. 1(b)], 1.08 [Fig. 1(d)], and 1.01 [Fig. 1(f)]. This illustrates that $F^{\lambda}_{\text{unitary}}$ makes best use of the information contained in the $d+1$ state fidelities, $F_{B,i}$ and F_{TR}. Bounds for over- and underestimating the gate error, obtained numerically, are presented in Table I with CNOT, identity, and the Toffoli gate as target operations. For three-qubit gates, we find the numerical bounds to be essentially contained by those for two-qubit gates (see Table I). This suggests our numerical bounds to be independent of system size. A verification of this conjecture for larger system sizes is, however, hampered by the enormous increase in numerical effort for randomization. For our examples of CNOT, the Toffoli gate, and identity, we find the estimated gate error based on Eqs. (8) to deviate from the standard one in the worst case by a factor smaller than 2.5 and on average by a factor smaller than 1.2. This confirms that $d+1$ state fidelities F_j are sufficient to accurately estimate the gate error.

B. Quantifying nonunitarity

If, in a given experimental setting, the gate error turns out to be larger than expected, one might want to know whether it is due to unitary errors or decoherence. This can be determined by quantifying nonunitarity of the time evolution using the following distance measure:

$$F_{\text{diss}} = 1 - \frac{1}{d+1}\left\{\sum_{i=1}^{d} \text{Tr}\left[\rho^2_{B,i}(T)\right] + \text{Tr}\left[\rho^2_{\text{TR}}(T)\right]\right\}, \quad (9)$$

where $\rho_j(T) = \mathcal{D}(\rho_j)$. $F_{\text{diss}} = 0$ if and only if the evolution is completely unitary. Evaluation of F_{diss} requires preparation of the $d+1$ input states of Eq. (3) and measurement of d^2+d populations.

Equation (9) cannot replace full process tomography when complete identification of the error sources is desired. However, some information can already be gained by inspection of the $d+1$ purities of Eq. (9). For example, if the purity loss is due to a single or very few terms in Eq. (9), this identifies the state evolutions that are subject to dissipation. On the other hand, if the purity loss is equally distributed over all basis states, the chosen basis is likely not an eigenbasis of the error operators (but another mutually unbiased basis presumably is).

IV. REDUCED SET OF STATES YIELDING ANALYTICAL BOUNDS ON THE AVERAGE FIDELITY

We now connect our notion of a reduced set of input states to the result of Ref. [11] that two classical fidelities can be used to obtain an upper and a lower bound on the average fidelity. The classical fidelity is given by the average probability of obtaining the correct output for each of the d classically possible input states:

$$F_c = \frac{1}{N}\sum_{i=1}^{d}\langle k_i^{(1)}|U_0^{\dagger}\mathcal{D}\big(|k_i^{(1)}\rangle\langle k_i^{(1)}|\big)U_0|k_i^{(1)}\rangle, \quad (10)$$

for an arbitrary orthonormal Hilbert-space basis $\{|k_i^{(1)}\rangle\}_{i=1,\ldots,d}$. It can be interpreted as the arithmetic average over the overlaps between expected and actual population evolution for the basis states $|k_i^{(1)}\rangle$. Defining $\rho_i^{(1)} = |k_i^{(1)}\rangle\langle k_i^{(1)}|$, such a classical fidelity can be rewritten analogously to Eq. (6):

$$\begin{aligned} F_1 &= \frac{1}{N}\sum_{i=1}^{d}\langle k_i^{(1)}|U_0\mathcal{D}\big(\rho_i^{(1)}\big)U_0^{\dagger}|k_i^{(1)}\rangle \\ &= \frac{1}{N}\sum_{ij=1}^{d}\langle k_j^{(1)}|k_i^{(1)}\rangle\langle k_i^{(1)}|U_0\mathcal{D}\big(\rho_i^{(1)}\big)U_0^{\dagger}|k_j^{(1)}\rangle \\ &= \frac{1}{N}\sum_{i=1}^{d}\text{Tr}\big[\rho_i^{(1)}U_0\mathcal{D}\big(\rho_i^{(1)}\big)U_0^{\dagger}\big] \\ &= \frac{1}{N}\sum_{i=1}^{d}\text{Tr}\big[U_0^{\dagger}\rho_i^{(1)}U_0\mathcal{D}\big(\rho_i^{(1)}\big)\big], \end{aligned}$$

with $U_0^{\dagger}\rho_i^{(1)}U_0$ the ideal and $\mathcal{D}(\rho_i^{(1)})$ the actual evolutions. In our terminology, the states $\rho_i^{(1)}$ "fix" the basis [see Eq. (3a)]. In order to fulfill the requirements of a reduced set, i.e., to allow for differentiating any two unitaries and assessing unitarity of the time evolution, another state corresponding to the totally rotated projector is necessary (see Sec. II). Instead of a single state ρ_{TR}, Ref. [11] chooses d such states with each state fulfilling the condition of total rotation: $\rho_i^{(2)} = |k_i^{(2)}\rangle\langle k_i^{(2)}|$ with

$$\big|\langle k_i^{(1)}|k_j^{(2)}\rangle\big|^2 = \frac{1}{d} \quad \forall i,j,$$

i.e., a complete mutually unbiased basis [16]. Evaluating the classical fidelities for the two bases $\{|k_i^{(1)}\rangle\}_{i=1,\ldots,d}$, $\{|k_i^{(2)}\rangle\}_{i=1,\ldots,d}$ then allows for analytical bounds on the average fidelity [11].

Note that Ref. [11] discusses a specific choice of the two bases. From our derivation in Sec. II, it is clear that any two mutually unbiased bases are suitable, and one can choose the most convenient ones. There exist $d+1=2^N+1$ mutually unbiased bases for N qubits [17], but only three of them consist of separable states while the remaining $d-2$ mutually unbiased bases are made up of maximally entangled states [10]. Any two of the three separable mutually unbiased bases constitute a natural choice for most experimental setups.

V. CONCLUSIONS

We have shown that a reduced set of input states can be used to estimate the average fidelity or gate error of a quantum gate. It provides the information to characterize, instead of the full open system evolution, only the unitary part. The average over all Hilbert space can then be estimated by a modified average over a reduced set of states that allows us to differentiate any two unitaries and quantify nonunitarity of the evolution. The states in the reduced set correspond to a complete set of orthonormal one-dimensional projectors plus a one-dimensional projector that is rotated with respect to all the other projectors. The reduced set can be realized by two mixed states, irrespective of the dimension d of the Hilbert space, or by $d+1$ pure states. Our concept of total rotation is related to the notion of mutually unbiased bases [16] where all states of the second basis are totally rotated with respect to the first basis. It is also the underlying principle in constructing the input states for two complementary classical fidelities [11]. Consequently, one can estimate the average fidelity using $d+1$ or $2d$ pure separable input states. In both cases, the gate error is determined in terms of state fidelities for the time-evolved states of the reduced set. The approach using $2d$ input states comes with the advantage of analytical bounds on the gate error. For the smaller set of $d+1$ input states, numerical calculations demonstrate the estimate to deviate from the true gate error by a factor of less than 1.2 on average and 2.5 in the worst case.

While the average gate fidelity currently enjoys great popularity, other very useful performance measures exist [18]. For example, the worst case fidelity is relevant in the context of the error correction threshold [19]. It would be interesting to see whether the $d+1$ or $2d$ state fidelities of the reduced set allow for estimating bounds on the worst case fidelity. This is, however, beyond the scope of our current work.

Another important question concerns the scaling of the gate error estimate employing a reduced set of states with the number of qubits. The straightforward but not most efficient approach consists in determining the required $d+1$ or $2d$ state fidelities by state tomography. This yields a scaling of 2^{3N} for standard state tomography and 2^{2N} for Monte Carlo state characterization [3,4], i.e., no improvement over current approaches. Alternatively, a reduced set of states can be combined with Monte Carlo process characterization [3,4]. We show in Ref. [20] that in this case the experimental effort and the classical computational resources to obtain tight analytical bounds on the average error are reduced by a factor of 2^N compared to the best currently available protocol for general unitary operations.

The ability to measure the gate performance efficiently with a reduced set of input states is not only a prerequisite for the development of quantum devices; it also opens the door to designing quantum gates in coherent control experiments using, e.g., genetic algorithms where repeated checks of the performance are required.

ACKNOWLEDGMENTS

We would like to thank Christian Roos for helpful comments. Financial support from the European Commission through the FP7-People Intra-European Fellowships Marie Curie action Grant No. PIEF-GA-2009-254174 is gratefully acknowledged.

APPENDIX: PROOFS

We provide here detailed proofs of the claims made in Sec. II.

1. Injectivity of $\mathcal{M}$ equivalent to the commutant space $\mathcal{K}(\{\rho_i\})$ having identity as its only element

Definition. Let ρ be a density operator defined in a d-dimensional Hilbert space and U_i elements of the projective unitary group $PU(d)$. We call the set of operators

$$K(\rho)=\{U_i\in PU(d)|[U_i,\rho]=0\}$$

the commutant space of ρ in $PU(d)$. The commutant space of a set of density operators $\{\rho_j\}$ is defined as

$$K(\{\rho_j\})=\bigcap_j K(\rho_j).$$

Proposition. The map $\mathcal{M}:PU(d)\rightarrow\bigoplus_i\mathbb{C}^{n\times n}$, which maps any unitary $U\in PU(d)$ to the set of propagated density operators $\{\rho_i^{(U)}(T)\}$, is injective if and only if the commutant space of $\{\rho_i\}$ in $PU(d)$, $\mathcal{K}(\{\rho_i\})$, contains only the identity.

Proof. Injectivity of $\mathcal{M}$ is equivalent to the condition

$$\forall i:\rho_i^{(U)}(T)=\rho_i^{(V)}(T)\Longleftrightarrow U=V.$$

We first show that this condition is equivalent to

$$\forall i:\rho_i^{(U)}(T)=\rho_i\Longleftrightarrow U=\mathbb{1}.$$

Assuming validity of $\forall i:\rho_i^{(U)}(T)=\rho_i^{(V)}(T)\Longleftrightarrow U=V$, just choose $V=\mathbb{1}$. Then $\rho_i^{(V)}(T)=\rho_i$ and the second statement follows immediately. Conversely, assume

$$\forall i:\rho_i^{(U)}(T)=\rho_i\Longleftrightarrow U=\mathbb{1}.$$

Then, for arbitrary $V,W\in PU(d)$ we set $U=V^{-1}W=V^+W$ and

$$\begin{aligned}\forall i:\rho_i^{(V^+W)}(T)=\rho_i&\Longleftrightarrow\forall i:V^+W\rho_iW^+V=\rho_i\\&\Longleftrightarrow\forall i:W\rho_iW^+=V\rho_iV^+\\&\Longleftrightarrow\forall i:\rho_i^{(W)}(T)=\rho_i^{(V)}(T).\end{aligned}$$

By assumption $\forall i:\rho_i^{(V^+W)}(T)=\rho_i\Longleftrightarrow V^+W=\mathbb{1}$, but since

$$\forall i:\rho_i^{(V^+W)}(T)=\rho_i\Longleftrightarrow\forall i:\rho_i^{(W)}(T)=\rho_i^{(V)}(T)$$

and the relation

$$V^{+}W = \mathbb{1} \Longleftrightarrow W = V$$

always holds for $V,W \in PU(d)$, this leads to the desired result: $\forall i : \rho_i^{(U)}(T) = \rho_i^{(V)}(T) \Longleftrightarrow U = V$.

We now show that $\mathcal{K}(\{\rho_i\}) = \mathbb{1}$ if and only if

$$\forall i : \rho_i^{(U)}(T) = \rho_i \Longleftrightarrow U = \mathbb{1}.$$

Consider the following calculation:

$$\begin{aligned}\forall i : \rho_i^{(U)}(T) = \rho_i &\Longleftrightarrow \forall i : U\rho_i U^{+} = \rho_i\\ &\Longleftrightarrow \forall i : U\rho_i = \rho_i U\\ &\Longleftrightarrow \forall i : U\rho_i - \rho_i U = 0\\ &\Longleftrightarrow \forall i : [U,\rho_i] = 0\\ &\overset{(*)}{\Longleftrightarrow} U = \mathbb{1}.\end{aligned}$$

The equivalence relation $(*)$ is true if and only if $\mathcal{K}(\{\rho_i\}) = \mathbb{1}$. This concludes the proof.

2. Total rotation and commutation with identity

Definition. Let $\mathcal{H}$ be a d-dimensional Hilbert space. A set $\mathcal{P}_c$ of d one-dimensional orthogonal projectors from $\mathcal{H}$ onto itself is called complete. For example, spanning the Hilbert space by an arbitrary complete orthonormal basis $\{|\varphi_i\rangle\}$, $\mathcal{P}_c = \{P_i = |\varphi_i\rangle\langle\varphi_i|\}$. A one-dimensional projector P_{TR} from $\mathcal{H}$ onto itself is called totally rotated with respect to the set $\mathcal{P}_c$ if $\forall P_i \in \mathcal{P}_c :\ P_{\text{TR}}P_i \neq 0$. A set $\mathcal{P}_{c\text{TR}} \equiv \{\mathcal{P}_c, P_{\text{TR}}\}$ of projectors is called complete and totally rotating.

Definition. Let $\mathcal{H}$ be a d-dimensional Hilbert space. A set of density operators $\{\rho_i\}$ with $\rho_i \in \mathcal{H}\otimes\mathcal{H}$ is called complete if the set of projectors on the eigenspaces of the $\{\rho_i\}$ is complete and is called complete and totally rotating if the set of projectors on the eigenspaces of the $\{\rho_i\}$ is complete and totally rotating.

Our goal is to prove that the only projective unitary matrix that commutes with each element of a complete and totally rotating set of states is the identity. In order to make use of the assumed commutation relations in the proof, we translate commutation of a unitary with a state into commutation of a unitary with one or more projectors. To this end, we introduce a lemma. Using commutation of a unitary with projectors, it is then straightforward to show that the unitary must be the identity.

Lemma. If $[U,\rho] = 0$ for a unitary $U \in PU(d)$ and a density operator ρ which has at least one nondegenerate eigenvalue λ_1, then $[U,P_1] = 0$ where P_1 is the projector onto the eigenspace $\mathcal{E}_1$ corresponding to the eigenvalue λ_1.

Proof. Since ρ has a nondegenerate eigenvalue λ_1, we can expand it in a set of orthonormal projectors, $\rho = \lambda_1 P_1 + \sum_{i=2}^{d}\lambda_i P_i$, with $P_1 = |\xi_1\rangle\langle\xi_1|$ the projector onto the one-dimensional eigenspace $\mathcal{E}_1$. By assumption,

$$\begin{aligned}[U,\rho] = 0 &= \lambda_1 U P_1 - \lambda_1 P_1 U + \sum_{i=2}^{d}(\lambda_i U P_i - \lambda_i P_i U)\\ &= \lambda_1 U P_1 U^{+} - \lambda_1 P_1 + \sum_{i=2}^{d}(\lambda_i U P_i U^{+} - \lambda_i P_i),\end{aligned}$$

where in the second line we have multiplied by U^{+} from the right. Defining $\bar{P}_i = U P_i U^{+}$, this is equivalent to

$$\lambda_1 \bar{P}_1 + \sum_{i=2}^{d}\lambda_i \bar{P}_i = \lambda_1 P_1 + \sum_{i=2}^{d}\lambda_i P_i.$$

The operator equality can be applied to $|\xi_1\rangle$, leading to

$$\lambda_1 \bar{P}_1 |\xi_1\rangle + \sum_{i=2}^{d}\lambda_i \bar{P}_i |\xi_1\rangle = \lambda_1 |\xi_1\rangle .$$

Inserting identity, $\sum_{i=1}^{d}\bar{P}_i = \mathbb{1}$, in the right-hand side, we obtain

$$\lambda_1 \bar{P}_1 |\xi_1\rangle + \sum_{i=2}^{d}\lambda_i \bar{P}_i |\xi_1\rangle = \lambda_1 \bar{P}_1 |\xi_1\rangle + \sum_{i=2}^{d}\lambda_1 \bar{P}_i |\xi_1\rangle .$$

Multiplying from the left by $\bar{P}_{i\neq 1}$ and using orthogonality of the $\bar{P}_i$ and nondegeneracy of λ_1, $\lambda_{i\neq 1} \neq \lambda_1$, we find that $\bar{P}_i|\xi_1\rangle = 0$ for all $i \neq 1$. Therefore $|\xi_1\rangle$ lies also in the one-dimensional eigenspace corresponding to $\bar{P}_1$, and the one-dimensional eigenspaces of P_1 and $\bar{P}_1$ must be identical. This implies

$$P_1 = \bar{P}_1,$$

and, by definition of $\bar{P}_1$, we find that U leaves the one-dimensional eigenspace corresponding to P_1 invariant and hence commutes with P_1.

Note that if a density operator ρ that commutes with U has more than one nondegenerate eigenvalue, the lemma implies commutation of U with all the projectors onto the one-dimensional eigenspaces.

Proposition. The only projective unitary matrix that commutes with a set of states $\{\rho_i\}$ that is complete and totally rotating is the identity.

Proof. Repeated application of the lemma to states ρ_i yields a set of one-dimensional projectors that each commute with U. By definition of a complete and totally rotating set of states, $d+1$ projectors within this set must be elements of $\{\mathcal{P}_c, P_{\text{TR}}\}$. We can thus choose the complete set of one-dimensional projectors $\mathcal{P}_c$ to represent U, $U = \sum_{i=1}^{d} u_i P_i$. An equally valid choice $\{\tilde{P}_i\}$ employs the totally rotated projector, $\tilde{P}_1 = P_{\text{TR}}$, with $\mathcal{E}_{\text{TR}}$ the corresponding eigenspace, and a suitable set of orthonormal one-dimensional projectors $\{\tilde{P}_i\}_{i=2,\ldots,d}$ for the space $\mathcal{E}_{\text{TR}}^{\perp}$ such that $U = \sum_{i=1}^{d} u_i \tilde{P}_i$. The spectrum $\{u_i\}$ is of course independent of the representation. Consider the action of U on a vector $|\zeta\rangle \in \mathcal{E}_{\text{TR}}$:

$$\begin{aligned}U|\zeta\rangle &= \sum_{i=1}^{d} u_i P_i |\zeta\rangle\\ &= \sum_{i=1}^{d} u_i \tilde{P}_i |\zeta\rangle = u_1 |\zeta\rangle = \sum_{i=1}^{d} u_1 P_i |\zeta\rangle , \qquad \text{(A1)}\end{aligned}$$

where we have inserted $\sum_{i=1}^{d} P_i = \mathbb{1}$ in the last step. By total rotation, $P_{\text{TR}}P_i \neq 0\ \forall P_i \in \mathcal{P}_c$, or equivalently, $P_i P_{\text{TR}} \neq 0$. Applying this to $|\zeta\rangle$, we find

$$P_i P_{\text{TR}} |\zeta\rangle = P_i |\zeta\rangle \neq 0 \quad \forall i.$$

Since the P_i are one-dimensional orthonormal projectors, i.e., $P_i = |\varphi_i\rangle\langle\varphi_i|$ with $\{|\varphi_i\rangle\}$ being a complete orthonormal basis of the Hilbert space, we can rewrite $P_i|\zeta\rangle$:

$$P_i|\zeta\rangle = \mu_i|\varphi_i\rangle,$$

with $\mu_i \in \mathbb{C}$, $\mu_i \neq 0$. Inserting this into Eq. (A1), we obtain

$$\sum_{i=1}^{d} u_1\mu_i|\varphi_i\rangle = \sum_{i=1}^{d} u_i\mu_i|\varphi_i\rangle.$$

Comparing the coefficients yields $u_1\mu_i = u_i\mu_i\ \forall i$. Since all $\mu_i \neq 0$ due to total rotation, we can divide and obtain

$$u_1 = u_i \quad \forall i,$$

i.e., a unitary with complete degeneracy in its eigenvalues. This necessarily has to be the matrix $e^{i\varphi}\mathbb{1}$ for $\varphi \in [0,2\pi]$ or, as an element of $PU(d)$, the unit matrix.

We have thus shown that only the identity commutes with a set of states that is complete and totally rotating. This set of states is therefore sufficient to differentiate any two unitaries.

3. Unitarity of $\mathcal{D}$ equivalent to projectors being mapped onto projectors

Proposition. A dynamical map $\mathcal{D}$, defined on a d-dimensional Hilbert space, is unitary if and only if $\mathcal{D}$ maps (i) a set $\{P_i\}$ of d one-dimensional orthonormal projectors onto a set of d one-dimensional orthonormal projectors $\{\tilde{P}_i\}$ and (ii) a one-dimensional projector that is totally rotated with respect to $\{P_i\}$ onto a one-dimensional projector (which is totally rotated with respect to $\{\tilde{P}_i\}$).

Proof. We first prove the forward direction. If the time evolution is unitary, the action of $\mathcal{D}$ on any state is described by $\mathcal{D}(\rho) = U\rho U^+$. Specifically for orthonormal projectors $P_iP_j = \delta_{ij}$, we find

$$\mathcal{D}(P_i)\mathcal{D}(P_j) = UP_iU^+UP_jU^\dagger = UP_iP_jU^\dagger = \delta_{ij}UP_iU^\dagger.$$

Since a one-dimensional projector can be written $P_i = |\varphi_i\rangle\langle\varphi_i|$, where $\{|\varphi_i\rangle\}$ is a complete orthonormal basis of $\mathcal{H}$, $UP_iU^\dagger$ is also one-dimensional projector. By the same argument, P_{TR} is mapped onto a one-dimensional projector if $\mathcal{D}(\rho) = U\rho U^+$. Therefore a dynamical map $\mathcal{D}$ describing unitary time evolution maps a set of d orthonormal projectors, $\{P_i\}$, onto another such set, $\{\tilde{P}_i = UP_iU^+\}$, and P_{TR} onto a one-dimensional projector.

We now prove the backward direction, starting from the representation of $\mathcal{D}$,

$$\mathcal{D} = \sum_{k=1}^{K} E_k\rho E_k^+, \tag{A2}$$

by Kraus operators E_k, i.e., linear operators that fulfill

$$\sum_{k=1}^{K} E_k^+E_k = \mathbb{1}. \tag{A3}$$

We employ the canonical representation in which the Kraus operators are orthogonal, $\mathrm{Tr}[E_k^+E_l] \sim \delta_{kl}$. By assumption, a set of d one-dimensional, orthonormal projectors $\{P_i\}$ is mapped by $\mathcal{D}$ onto another such set $\{\tilde{P}_i\}$:

$$\mathcal{D}(P_i) = \sum_{k=1}^{K} E_kP_iE_k^+ = \tilde{P}_i. \tag{A4}$$

We need to show that this implies $\mathcal{D}(\rho) = U\rho U^+$ or equivalently, as we demonstrate below, that $\mathcal{D}$ is made up of a single Kraus operator E_1 in the representation where $\mathrm{Tr}[E_k^+E_l] \sim \delta_{kl}$. In general, we can employ a polar decomposition for each Kraus operator, factorizing it into a unitary and a positive-semidefinite operator, $E_k = U_k\tilde{E}_k$. For unitary evolution, $U_k = \tilde{U}$ for all k and $E_1 = U\mathbb{1}$, which is a special case of $\tilde{E}_k$ being diagonal. We first show that the assumption for the d orthonormal projectors $\{P_i\}$ implies $U_k = \tilde{U}$ and diagonality of $\tilde{E}_k$. In a second step, we prove that the assumption for the totally rotated projector implies that there is only a single Kraus operator and $\tilde{E}_1 = \mathbb{1}$.

We first show that $\tilde{E}_k = E_kU^+$ is diagonal in the orthonormal basis $\{|\varphi_i\rangle\}$ corresponding to the P_i. Equation (A4) suggests the definition of an operator $\Pi_k^{(i)} \equiv E_kP_iE_k^+$ which is obviously Hermitian and moreover semipositive definite. The latter is seen by making use of $P_i^2 = P_i$ and $P_i = P_i^+$: $\langle\zeta|\Pi_k^{(i)}\zeta\rangle = \langle\zeta|E_kP_iP_iE_k^+\zeta\rangle = \langle P_iE_k^+\zeta|P_iE_k^+\zeta\rangle = \langle\xi|\xi\rangle \geqslant 0$ for any $|\zeta\rangle \in \mathcal{H}$. Equation (A4) implies $\sum_{k=1}^{K}\Pi_k^{(i)} = \tilde{P}_i$. For the normalized vector spanning the eigenspace of $\tilde{P}_i$, $|\tilde{\varphi}_i\rangle \in \mathcal{E}_i$, we find

$$\sum_{k=1}^{K}\langle\tilde{\varphi}_i|\Pi_k^{(i)}\tilde{\varphi}_i\rangle = 1,$$

while for all $|\xi\rangle \in \mathcal{E}_i^\perp$

$$\sum_{k=1}^{K}\langle\xi|\Pi_k^{(i)}\xi\rangle = 0.$$

Due to positive semidefiniteness of $\Pi_k^{(i)}$, this implies $\langle\xi|\Pi_k^{(i)}\xi\rangle = 0$. Reinserting the definition of $\Pi_k^{(i)}$ leads to $\langle\xi|E_kP_iE_k^+\xi\rangle = \langle P_iE_k^+\xi|P_iE_k^+\xi\rangle = 0$; i.e., we find $P_iE_k^+|\xi\rangle = 0$ for all k, i and $|\xi\rangle \in \mathcal{E}_i^\perp$. For an arbitrary Hilbert-space vector $|\zeta\rangle$, $(\mathbb{1} - \tilde{P}_i)|\zeta\rangle$ lies in $\mathcal{E}_i^\perp$ such that $P_iE_k^+(\mathbb{1} - \tilde{P}_i)|\zeta\rangle = 0$ for all k and i. Therefore,

$$P_iE_k^+(\mathbb{1} - \tilde{P}_i) = 0, \quad \text{or} \quad P_iE_k^+ = P_iE_k^+\tilde{P}_i \quad \forall i,k.$$

To make use of the orthogonality of the $\tilde{P}_i$, we multiply by $\tilde{P}_j$, $j \neq i$ from the right. Since $\tilde{P}_j$ can be written as $\tilde{P}_j = \tilde{U}P_j\tilde{U}^+$ for a specific $\tilde{U}$, we obtain, for all i, k, and $j \neq i$, $P_iE_k^+\tilde{U}P_j\tilde{U}^+ = 0$. Multiplication by $\tilde{U}$ from the right yields

$$P_iE_k^+\tilde{U}P_j = 0.$$

This implies that the operators $E_k^+\tilde{U}$ have to be diagonal in the basis corresponding to the P_i:

$$E_k^+\tilde{U} = \sum_{i=1}^{d} e_i^kP_i. \tag{A5}$$

Note that the unitary $\tilde{U}$ is the same for all Kraus operators E_k.

In the second step, we now need to show that the right-hand side of Eq. (A5) is equal to the identity, making use of the assumption that the totally rotated projector is mapped by $\mathcal{D}$ onto a one-dimensional projector. The crucial information is captured in the coefficients e_i^k. Let us summarize what we know about the e_i^k. From orthogonality of the Kraus operators, we find $\mathrm{Tr}[E_k^+ E_l] = \mathrm{Tr}[\sum_{i,j=1}^d e_i^k (e_j^l)^* P_i \tilde{U}^+ \tilde{U} P_j] = \sum_{i,j=1}^d e_i^k (e_j^l)^* \mathrm{Tr}[P_i P_j] = \sum_{i,j=1}^d e_i^k (e_j^l)^* \delta_{ij} = \sum_{i=1}^d e_i^k (e_i^l)^* \overset{!}{\sim} \delta_{kl}$. The last sum can be interpreted as a scalar product for two orthogonal vectors $\vec{e}^{\,k}, \vec{e}^{\,l} \in \mathbb{C}^d$ with coefficients e_i^k, e_i^l. Defining the proportionality constants $\mathcal{N}(k)$,

$$\mathcal{N}(k) \equiv \mathrm{Tr}[E_k^+ E_k] = \sum_i e_i^k \left(e_i^k\right)^* = \langle \vec{e}^{\,k}, \vec{e}^{\,k} \rangle \geqslant 0, \quad \text{(A6)}$$

we find from Eq. (A3) and $\mathrm{Tr}[\mathbb{1}] = d$ that $\sum_{k=1}^K \mathcal{N}(k) = d$ [and, if we can show that $\mathcal{N}(k) = d$ for one k, then the number of Kraus operators, K, must be 1]. Equation (A3) together with Eq. (A5) yields yet another condition on the e_i^k: $\mathbb{1} = \sum_{k=1}^K E_k^+ E_k = \sum_{i,j=1}^d \sum_{k=1}^K (e_i^k)^* e_j^k P_i P_j = \sum_{i,k} |e_i^k|^2 P_i$ such that $\sum_k |e_i^k|^2 = 1$ for each i. This can be interpreted as a normalization condition for a vector $\vec{\epsilon}_i \in \mathbb{C}^K$ with coefficients e_i^k:

$$1 = \sum_{k=1}^K \left|e_i^k\right|^2 = \langle \vec{\epsilon}_i, \vec{\epsilon}_i \rangle. \quad \text{(A7)}$$

Since the vector sets $\{\vec{e}_k\}$ and $\{\vec{\epsilon}_i\}$ are not independent, it is clear that any information on the scalar product $\langle \vec{\epsilon}_i, \vec{\epsilon}_j \rangle$ will be useful to determine $\mathcal{N}(k)$ (such that we can check whether there is one k for which $\mathcal{N}(k) = d$). To this end, we employ the assumption that P_{TR} is mapped by $\mathcal{D}$ onto a one-dimensional projector, $\tilde{P}_{\mathrm{TR}} = \mathcal{D}(P_{\mathrm{TR}})$, or, in other words the purity of P_{TR} is preserved:

$$\mathrm{Tr}\{[\mathcal{D}(P_{\mathrm{TR}})]^2\} = 1.$$

Inserting Eqs. (A2) and (A5), making use of the orthogonality of the P_i and of the trace being invariant under cyclic permutation, we find

$$\begin{aligned}
&\mathrm{Tr}[\mathcal{D}(P_{\mathrm{TR}})^2] \\
&= \mathrm{Tr}\left[U\left(\sum_{ij}\sum_k\sum_{i'j'}\sum_{k'} \left(e_i^k\right)^* e_j^k \left(e_{i'}^{k'}\right)^* \right.\right. \\
&\quad \left.\left. \times\, e_{j'}^{k'} P_i P_{\mathrm{TR}} P_j P_{i'} P_{\mathrm{TR}} P_{j'}\right) U^+\right] \\
&= \mathrm{Tr}\left[\sum_{ij}\sum_k\sum_{j'}\sum_{k'} \left(e_i^k\right)^* e_j^k \left(e_j^{k'}\right)^* e_{j'}^{k'} P_i P_{\mathrm{TR}} P_j P_{\mathrm{TR}} P_{j'}\right] \\
&= \sum_{ij}\sum_k\sum_{j'}\sum_{k'} \left(e_i^k\right)^* e_j^k \left(e_j^{k'}\right)^* e_{j'}^{k'} \mathrm{Tr}[P_i P_{\mathrm{TR}} P_j P_{\mathrm{TR}} P_{j'}] \\
&= \sum_{ij}\left|\sum_k \left(e_i^k\right)^* e_j^k\right|^2 \mathrm{Tr}[P_i P_{\mathrm{TR}} P_j P_{\mathrm{TR}}] \\
&= \sum_{ij} |\langle \vec{\epsilon}_i, \vec{\epsilon}_j \rangle|^2 \mathrm{Tr}[P_i P_{\mathrm{TR}} P_j P_{\mathrm{TR}}].
\end{aligned}$$

The trace over the projectors is easily evaluated in the basis $\{|\varphi_i\rangle\}$, $P_i = |\varphi_i\rangle\langle\varphi_i|$, in which $P_{\mathrm{TR}} = |\Psi\rangle\langle\Psi|$. It yields $\mathrm{Tr}[P_i P_{\mathrm{TR}} P_j P_{\mathrm{TR}}] = |\langle\varphi_i|\Psi\rangle|^2 |\langle\varphi_j|\Psi\rangle|^2 = |\mu_i|^2|\mu_j|^2$ with $\mu_i \equiv \langle\varphi_i|\Psi\rangle$ and $\mu_i \neq 0$ due to total rotation, $P_i P_{\mathrm{TR}} \neq 0 \forall i$. Estimating $|\langle\vec{\epsilon}_i, \vec{\epsilon}_j\rangle|^2$ by the Cauchy Schwartz inequality, $|\langle\vec{\epsilon}_i, \vec{\epsilon}_j\rangle|^2 \leqslant \langle\vec{\epsilon}_i, \vec{\epsilon}_i\rangle\langle\vec{\epsilon}_j, \vec{\epsilon}_j\rangle$, and making use of the normalization of $\vec{\epsilon}_i$ [see Eq. (A7)], we obtain

$$\begin{aligned}
1 = \mathrm{Tr}[\mathcal{D}(P_{\mathrm{TR}})^2] &= \sum_{ij} |\mu_i|^2 |\mu_j|^2 |\langle\vec{\epsilon}_i, \vec{\epsilon}_j\rangle|^2 \\
&\leqslant \sum_{ij} |\mu_i|^2 |\mu_j|^2 = 1.
\end{aligned}$$

In the last step, we have used $\sum_i |\mu_i|^2 = \sum_i |\langle\varphi_i|\Psi\rangle|^2 = \sum_i \langle\Psi|\varphi_i\rangle\langle\varphi_i|\Psi\rangle = \langle\Psi|\Psi\rangle = 1$. Since we find one on the left-hand and right-hand sides, equality must hold for the inequality. Since $\mu_i \neq 0$ for all i, this is possible only for

$$|\langle\vec{\epsilon}_i, \vec{\epsilon}_j\rangle|^2 = 1, \quad \text{or} \quad |\langle\vec{\epsilon}_i, \vec{\epsilon}_j\rangle| = 1 \quad \forall i, j.$$

Therefore, the normalized vectors $\vec{\epsilon}_i$, $\vec{\epsilon}_j$ are identical up to a complex scalar, $|e_i^k| = |e_j^k|$ for all i, j, and k. This implies for the proportionality constants $\mathcal{N}(k)$, Eq. (A6), equality of all summands:

$$\mathcal{N}(k) = \sum_{i=1}^d e_i^k \left(e_i^k\right)^* = d\ \left(e_a^k\right)^* e_a^k.$$

Each component is thus given by $e_i^k = \sqrt{\mathcal{N}(k)/d}\exp[i\phi_i]$, which, making use of the orthogonality of the vectors $\vec{e}_k$, $\sum_i e_i^k (e_i^l)^* \sim \delta_{kl}$, leads to

$$\begin{aligned}
\sum_{i=1}^d e_i^k \left(e_i^l\right)^* &= \sum_{i=1}^d \frac{\sqrt{\mathcal{N}(k)\mathcal{N}(l)}}{d} \exp[i\phi_i]\exp[-i\phi_i] \\
&= \sqrt{\mathcal{N}(k)\mathcal{N}(l)} = 0 \quad \forall k \neq l.
\end{aligned}$$

For this to be true, all $\mathcal{N}(k)$ except one and consequently all E_k except one must be zero. By Eq. (A5), its representation is

$$E = \tilde{U}\left[\sum_i \left(e_i^1\right)^* P_i\right].$$

Making use of $P_i P_j = \delta_{ij} P_i$ and $P_i = P_i^+$, unitarity of the time evolution follows immediately, since

$$\begin{aligned}
E^+ E &= \sum_{i=1}^d e_i^1 \left(e_i^1\right)^* P_i = \sum_{i=1}^2 \sqrt{\frac{\mathcal{N}(1)}{d}} P_i = \sum_{i=1}^k P_i = \mathbb{1}, \\
E E^+ &= \tilde{U}\left(\sum_{i=1} e_i^1 \left(e_i^1\right)^* P_i\right)\tilde{U}^+ = \tilde{U}\mathbb{1}\tilde{U}^+ = \mathbb{1},
\end{aligned}$$

such that

$$\mathcal{D}(\rho) = \tilde{U}\rho\tilde{U}^+$$

for a unitary $\tilde{U} \in PU(d)$. This concludes the proof.

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
[2] M. Mohseni, A. T. Rezakhani, and D. A. Lidar, Phys. Rev. A **77**, 032322 (2008).
[3] S. T. Flammia and Y.-K. Liu, Phys. Rev. Lett. **106**, 230501 (2011).
[4] M. P. da Silva, O. Landon-Cardinal, and D. Poulin, Phys. Rev. Lett. **107**, 210404 (2011).
[5] A. Shabani, R. L. Kosut, M. Mohseni, H. Rabitz, M. A. Broome, M. P. Almeida, A. Fedrizzi, and A. G. White, Phys. Rev. Lett. **106**, 100401 (2011).
[6] C. T. Schmiegelow, A. Bendersky, M. A. Larotonda, and J. P. Paz, Phys. Rev. Lett. **107**, 100502 (2011).
[7] M. Mohseni and A. T. Rezakhani, Phys. Rev. A **80**, 010101 (2009).
[8] L. Steffen, M. P. da Silva, A. Fedorov, M. Baur, and A. Wallraff, Phys. Rev. Lett. **108**, 260506 (2012).
[9] A. Bendersky, F. Pastawski, and J. P. Paz, Phys. Rev. Lett. **100**, 190403 (2008).
[10] J. Lawrence, Phys. Rev. A **84**, 022338 (2011).
[11] H. F. Hofmann, Phys. Rev. Lett. **94**, 160504 (2005).
[12] B. P. Lanyon *et al*., Science **334**, 57 (2011).
[13] S. Kallush and R. Kosloff, Phys. Rev. A **73**, 032324 (2006).
[14] J. A. Miszczak, Z. Puchała, and P. Gawron, *Quantum Information Package for Mathematica*, http://zksi.iitis.pl/wiki/projects:mathematica-qi.
[15] F. Mezzadri, Notices of the AMS **54**, 592 (2007), available online at http://www.ams.org/notices/200705/.
[16] A. Fernández-Pérez, A. B. Klimov, and C. Saavedra, Phys. Rev. A **83**, 052332 (2011).
[17] W. K. Wootters and B. D. Fields, Ann. Phys. **191**, 363 (1989).
[18] A. Gilchrist, N. K. Langford, and M. A. Nielsen, Phys. Rev. A **71**, 062310 (2005).
[19] C. Bény and O. Oreshkov, Phys. Rev. Lett. **104**, 120501 (2010).
[20] D. M. Reich, G. Gualdi, and C. P. Koch, arXiv:1305.5649.