Editors' Suggestion

Recovering Quantum Gates from Few Average Gate Fidelities

I. Roth,[1,*] R. Kueng,[2] S. Kimmel,[3] Y.-K. Liu,[4,5] D. Gross,[6] J. Eisert,[1,9] and M. Kliesch[7,8,†]

[1]*Dahlem Center for Complex Quantum Systems, Physics Department, Freie Universität Berlin, D-14195 Berlin, Germany*
[2]*Institute for Quantum Information and Matter, California Institute of Technology, Pasadena, California 91125, USA*
[3]*Department of Computer Science, Middlebury College, Middlebury, Vermont 05753, USA*
[4]*National Institute of Standards and Technology, Gaithersburg, Maryland 20899, USA*
[5]*Joint Center for Quantum Information and Computer Science (QuICS), University of Maryland, College Park, Maryland 20742, USA*
[6]*Institute for Theoretical Physics, University of Cologne, D-50937 Cologne, Germany*
[7]*Institute of Theoretical Physics and Astrophysics, National Quantum Information Centre, University of Gdańsk, 80-308 Gdańsk, Poland*
[8]*Institute for Theoretical Physics, Heinrich Heine University Düsseldorf, D-40225 Düsseldorf, Germany*
[9]*Institute of Mathematics and Computer Science, Freie Universität Berlin, D-14195 Berlin, Germany*

(Received 5 May 2018; published 24 October 2018)

Characterizing quantum processes is a key task in the development of quantum technologies, especially at the noisy intermediate scale of today's devices. One method for characterizing processes is randomized benchmarking, which is robust against state preparation and measurement errors and can be used to benchmark Clifford gates. Compressed sensing techniques achieve full tomography of quantum channels essentially at optimal resource efficiency. In this Letter, we show that the favorable features of both approaches can be combined. For characterizing multiqubit unitary gates, we provide a rigorously guaranteed and practical reconstruction method that works with an essentially optimal number of average gate fidelities measured with respect to random Clifford unitaries. Moreover, for general unital quantum channels, we provide an explicit expansion into a unitary 2-design, allowing for a practical and guaranteed reconstruction also in that case. As a side result, we obtain a new statistical interpretation of the unitarity—a figure of merit characterizing the coherence of a process.

DOI: 10.1103/PhysRevLett.121.170502

As increasingly large and complex quantum devices are being built and the development of fault-tolerant quantum computation is moving forward, it is critical to develop tools to refine our control of these devices. For this purpose, several improved methods for characterizing quantum processes have been developed in recent years.

These improvements can be grouped into two broad categories. The first category includes techniques such as randomized benchmarking (RB) [1–11] and gate set tomography (GST) [12], which are more robust to state preparation and measurement (SPAM) errors. These techniques work by performing long sequences of random quantum operations, measuring their outcomes, and checking whether the resulting statistics are consistent with some physically plausible model of the system. In this way, one can characterize a quantum gate in terms of other quantum gates in a way that is insensitive to SPAM errors. The amount of information extracted by such techniques is extremely different. While RB typically characterizes a quantum gate in terms of a single fidelity, GST yields a complete description of an entire gate set, the state preparation, and the measurement. In effect, the data acquisition for GST requires an exceedingly large effort.

The second category [13–17] provides detailed tomographic information in a more resource-efficient way. It includes techniques such as compressed sensing [18–24], matrix product state tomography [25,26], and learning of local Hamiltonians and tensor network states [27,28]. These methods exploit the sparse, low-rank or low entanglement structure that is present in many of the physical states and processes that occur in nature. These techniques are less resource intensive than conventional tomography and therefore can be applied to larger numbers of qubits. Convex optimization techniques, such as semidefinite programming, are then used to reconstruct the underlying quantum state or process.

A recent line of work [29,30] has attempted to unify these two approaches to a quantum process tomography scheme that is both robust to SPAM errors and can handle large numbers of qubits (provided the quantum process has some suitable structure). To achieve this goal, it turns out that the proper design of the measurements is crucial. SPAM-robust methods such as randomized benchmarking are known to require some kind of computationally tractable group structure, such as that found in the Clifford group. Subsequently, RB methods were extended to other groups [31–35]. In this Letter we focus on the Clifford group. Clifford gates are motivated by their abundant appearance in many practical applications, such as fault-tolerant quantum computing [7,36].

In contrast, compressed sensing methods typically require measurements with less structure in this context, in that their fourth-order moments are close to those of the uniform Haar measure. Thus, the key technical question is whether the seemingly conflicting requirements of sufficient randomness and desired structure in the measurements can be combined.

In this work, we show that the answer is indeed yes. In layman's terms, we demonstrate that Clifford-group-based measurements are also sufficiently unstructured that they can be used for compressed sensing. Thus, we develop methods for quantum process tomography that are resource efficient, robust with respect to SPAM and other errors, and use measurements that are already routinely acquired in many experiments.

In more detail, we provide procedures for the reconstruction from so-called average gate fidelities (AGFs), which are the quantities that are measured in randomized benchmarking. It was established that the unital part of general quantum channels can be reconstructed from AGFs relative to a maximal linearly independent subset of Clifford-group operations [29]. We generalize this result by noting that the Clifford group can be replaced by an arbitrary unitary 2-design and also explicitly provide an analytic form of the reconstruction.

Our main result is a practical reconstruction procedure for quantum channels that are close to being unitary. Let d be the Hilbert space dimension, so that a unitary quantum channel can be described by roughly d^2 scalar parameters. The protocol is rigorously guaranteed to succeed using essentially order of d^2 AGFs with respect to randomly drawn Clifford gates, and we also prove it to be stable against errors in the AGF estimates. In this way, we generalize a previous recovery guarantee [30] from AGFs with 4-designs to ones with the more relevant Clifford gates.

Conversely, we prove that the sample complexity of our reconstruction procedure is optimal in a simplified measurement setting. Here, we assume that independent copies of the channel's Choi state are measured and use direct fidelity estimation [27,37] and information theoretic arguments [13] to show that the dimensional scaling of our reconstruction error is optimal up to log-factors. As a side result, we also find a new interpretation of the *unitarity* [8] —a figure of merit that captures the coherence of noise. We show that this quantity can be estimated directly from AGFs rather than simulating purity measurements [8].

In summary, we provide a protocol for quantum process tomography that fulfills all of the following desiderata: (i) It is based on physically reasonable and feasible measurements, (ii) makes use of them in a sample optimal fashion, (iii) exploits the structure of the expected or targeted channel (here, low Kraus rank reflecting quantum gates), and (iv) is stable against SPAM and other possible errors. In this sense, we expect our scheme to be of high importance and practically useful in actual experimental settings in future quantum technologies [38]. It adds to the information obtained from mere randomized benchmarking in that it provides actionable advice, especially regarding coherent errors. Such advice is particularly relevant for fault-tolerant quantum computation: Refs. [39,40] indicate that it is coherent errors that lead to an enormous mismatch between average errors, which are estimated by randomized benchmarking and worst-case errors reflected by fault-tolerance thresholds.

Our main technical contributions are results for the second and fourth moments of AGF measurements with random Clifford gates. For the second moment, we provide an explicit formula improving over the previous lower bound [30]. In the case of trace-preserving and unital maps, our analysis gives rise to a tight frame condition. In order to prove a bound on the fourth moment, we derive—as a more universal new technical tool—a general integration formula for the fourth-order diagonal tensor representation of the Clifford group. The proof builds on recent results on the representation theory of the multiqubit Clifford group [41–43]. Our result is the Clifford analogue to Collins's integration formula for the unitary group [44,45] for fourth orders, which we expect to also be useful in other applications. In the following, we present the precise formulation of our results. The proofs and technical contributions are given in the Supplemental Material [46].

A linear map from the set of Hermitian operators on a d-dimensional Hilbert space to itself is referred to as *map*. A quantum channel is a completely positive map that in addition preserves the trace of a Hermitian operator and, thus, maps quantum states to quantum states. A map is unital if the identity operator (equivalently, the maximally mixed state) is a fixed point of the map. We define the AGF between a map $\mathcal{X}$ and a quantum gate (i.e., a unitary quantum channel) $\mathcal{U}: \rho \mapsto U\rho U^\dagger$ associated with a unitary matrix $U \in U(d)$ as

$$F_{\mathrm{avg}}(\mathcal{U}, \mathcal{X}) = \int d\psi \langle\psi|U^\dagger \mathcal{X}(|\psi\rangle\langle\psi|)U|\psi\rangle, \qquad (1)$$

where the integral is taken according to the uniform (Haar) measure on state vectors.

The Clifford group constitutes a particularly important family of unitary gates that are featured prominently in state-of-the-art quantum architectures. Moreover, it was shown that for many-qubit systems (i.e., $d = 2^n$), any unital and trace-preserving map is fully characterized by its AGFs (1) with respect to the Clifford group [29]. A detailed analysis of the geometry of unital channels was previously given in Ref. [62]. There, it was shown that a quantum channel is unital if and only if it can be written as an affine combination of unitary gates. (*Affine* here means that the expansion coefficients sum to 1. Unlike *convex* combinations, they are, however, not restricted to being non-negative.) Motivated by the result for Clifford gates, one can ask more generally: What are the sets of unitary gates that span the set of unital and trace-preserving maps?

A general answer to this question can be given using the notion of unitary t-designs. Unitary t-designs [3,63] (and their state cousins, spherical t-designs [64,65], respectively) are discrete subsets of the unitary group $U(d)$ (resp., complex unit sphere) that are evenly distributed in the sense that their average reproduces the Haar (resp., uniform) measure over the full unitary group (resp., complex unit sphere) up to the tth moment. The multiqubit Clifford group, for example, forms a unitary 3-design [66–68]. For spherical designs, a close connection between informational completeness for quantum state estimation and the notion of a 2-design has been established in Ref. [65]; see also Refs. [69–71]. A similar result holds for quantum process estimation, and it is the starting point of our work. Indeed, the following is essentially due to Ref. [72]. We give a concise proof in the form of the slightly more general Theorem S.36 in the Supplemental Material [46].

Proposition 1. (Informational completeness and unitary designs) Let $\{\mathcal{U}_k\}_{k=1}^N$ be the gate set of a unitary 2-design represented as channels. Every unital and trace-preserving map $\mathcal{X}$ can be written as an affine combination $\mathcal{X} = (1/N)\sum_{k=1}^N c_k(\mathcal{X})\mathcal{U}_k$ of the $\mathcal{U}_k$'s. The coefficients are given by $c_k(\mathcal{X}) = CF_{\mathrm{avg}}(\mathcal{U}_k, \mathcal{X}) - (C/d) + 1$, where $C = d(d+1)(d^2 - 1)$.

Hence, every unital and trace-preserving map is uniquely determined by the AGFs with respect to an arbitrary unitary 2-design.

Clifford gates are a particularly prominent gate set with this 2-design feature. However, its cardinality scales superpolynomially in the dimension d. For explicit characterizations, this is far from optimal. However, in certain dimensions there exist subgroups of the Clifford group with cardinality proportional to d^4 that also form a 2-design [63,73]. More generally, order of $d^4 \log(d)$ Clifford gates drawn independent and identically distributed (i.i.d.) from the uniform distribution are an approximate 2-design [74]. From Proposition 1, we expect that such randomly generated approximate 2-designs yield approximate reconstruction schemes for unital channels.

Our main result focuses on the particular task of reconstructing multiqubit unital channels that are close to being unitary, i.e., well approximated by a channel of Kraus rank equal to 1. Techniques from low-rank matrix reconstruction [13,14,18,19,24,75] allow for exploiting this additional piece of information in order to reduce the number of AGFs required to uniquely reconstruct an unknown unitary gate.

Suppose we are given a list of m AGFs

$$f_i = F_{\mathrm{avg}}(\mathcal{C}_i, \mathcal{X}) + \epsilon_i, \qquad (2)$$

between the unknown unitary gate $\mathcal{X}$ and Clifford gates $\mathcal{C}_i$, where the $\mathcal{C}_i$ are chosen uniformly at random and the AGFs f_i are possibly corrupted by additive noise ϵ_i. In order to reconstruct $\mathcal{X}$ from these observations, we propose to perform a least-squares fit over the set of unital quantum channels, i.e.,

$$\begin{aligned} &\text{minimize} \sum_{i=1}^m [F_{\mathrm{avg}}(\mathcal{C}_i, \mathcal{Z}) - f_i]^2 \\ &\text{subject to } \mathcal{Z} \text{ is a unital quantum channel.} \end{aligned} \qquad (3)$$

We emphasize that this is an efficiently solvable convex optimization problem. The feasible set is convex since it is the intersection of an affine subspace (unital and trace-preserving maps) and a convex cone (completely positive maps).

Valid for multiqubit gates ($d = 2^n$), our main result states that this reconstruction procedure is guaranteed to succeed with exponentially high probability, provided that the number m of AGFs is proportional [up to a $\log(d)$-factor] to the number of degrees of freedom in a general unitary gate. The error of the reconstructed channel is measured with the Frobenius norm in Choi representation $\|\cdot\|$; see the Supplemental Material [46] for details. Here, we give a concise statement for the case of unitary gates. A more general version—Theorem S.16 in the Supplemental Material [46]—shows that the result can be extended to cover approximately unitary channels.

Theorem 2. (Recovery guarantee for unitary gates) Fix the dimension $d = 2^n$. Then,

$$m \geq cd^2 \log(d) \qquad (4)$$

noisy AGFs with randomly chosen Clifford gates suffice with high probability (of at least $1 - e^{-\gamma m}$) to reconstruct *any* unitary quantum channel $\mathcal{X}$ via Eq. (3). This reconstruction is stable in the sense that the minimizer $\mathcal{Z}^\sharp$ of Eq. (3) is guaranteed to obey

$$\|\mathcal{Z}^\sharp - \mathcal{X}\| \leq \tilde{C}\frac{d^2}{\sqrt{m}}\|\epsilon\|_{\ell_2}. \qquad (5)$$

The constants $\tilde{C}, c, \gamma > 0$ are independent of d.

We note the following:

(i) Equation (5) shows the protocol's inherent stability to additive noise. This stability combined with the robustness of randomized benchmarking against SPAM errors results in an estimation procedure that is potentially more resource intensive but considerably less susceptible to experimental imperfections and systematic errors than many other reconstruction protocols [13,16,37].

(ii) The proof can be verbatim adapted to an optimization of the ℓ_1 norm instead of the ℓ_2 norm in Eq. (3), resulting in a slightly stronger error bound.

(iii) The theorem achieves a quadratic improvement (up to a log-factor) over the minimal number of AGFs required

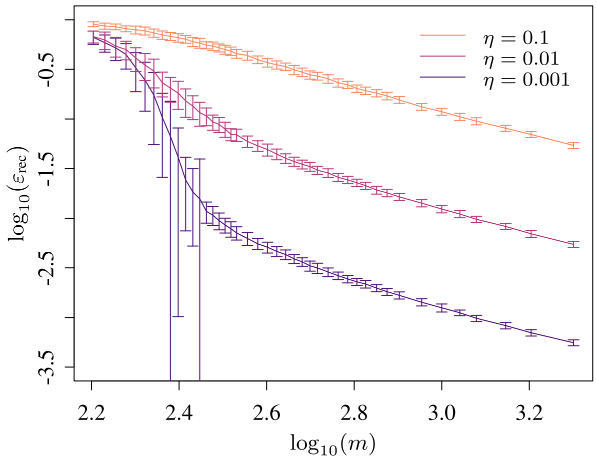

FIG. 1. Reconstruction of a Haar-random 3-qubit channel using the optimization (3): The plots show the dependence of the observed average reconstruction error $\varepsilon_{\rm rec} := \|\mathcal{Z}^\sharp - \mathcal{X}\|$ on the number of AGFs m for different noise strengths $\eta := \|\epsilon\|_{\ell_2}$. The error bars denote the observed standard deviation. The averages are taken over 100 samples of random i.i.d. measurements and channels (nonuniform). The MATLAB code and data used to create these plots can be found on GitHub [76].

for a naive reconstruction via linear inversion for the case of noiseless measurements. But what is the number of measurements required to obtain the AGFs and to suppress the effect of the measurement noise ϵ in the reconstruction error (5)? For randomized benchmarking setups, a fair accounting of all involved errors is beyond the scope of the current work. But in order to show that the scaling of the noise term in our reconstruction error (5) is essentially optimal, we consider the conceptually simpler measurement setting where the channel's Choi state is measured directly. In the Supplemental Material [46] E, we prove upper and lower bounds to the minimum number of channel uses sufficient for a reconstruction via algorithm (3) with reconstruction error (5) bounded by $\varepsilon_{\rm rec} > 0$. This number of channel uses scales as $d^4/\varepsilon_{\rm rec}^2$ up to log-factors. The upper bound relies on direct fidelity estimation [37]. In order to establish a lower bound, we extend information theoretic arguments from Ref. [13] to rank-1 measurements.

(iv) Finally, we note that the reconstruction (3) can be practically calculated using standard convex optimization packages. A numerical demonstration is shown in Fig. 1 and discussed in more detail in the Supplemental Material [46] H. There, we also show that measuring AGFs with respect to Clifford unitaries seems to be comparable to Haar-random measurements, even in the presence of noise. This confirms an observation that was already mentioned in Ref. [30].

The proof of Theorem 2 is presented in the Supplemental Material [46] D. The AGFs can be interpreted as expectation values of certain observables, which are unit rank projectors onto directions that correspond to elements of the Clifford group. In contrast, most previous work on tomography via compressed sensing features observables that have full rank, e.g., tensor products of Pauli operators. Since we now want to utilize observables that have unit rank, a different approach is needed. One approach developed by a subset of the authors in Ref. [30] is to use strong results from low-rank matrix reconstruction and phase retrieval [24,71,77–79]. These methods [24,79] require measurements that look sufficiently random and unstructured, in that their fourth-order moments are close to those of the uniform Haar measure. The multiqubit Clifford group, however, does constitute a 3-design, but not a 4-design. In Ref. [30], this discrepancy is partially remedied by imposing additional constraints (a "nonspikiness condition"; see also Ref. [80]) on the unitary channels to be reconstructed. In turn, their result also required these constraints to be included in the algorithmic reconstruction which renders the algorithm impractical [81]. Moreover, important classes of channels, e.g., Pauli channels, do not satisfy this condition in general. Here, we overcome these issues by appealing to recent works that fully characterize the fourth moments of the Clifford group [41,42]. In order to apply these results, we develop an integration formula for fourth moments over the Clifford group. This formula is analogous to the integration over the unitary group know as Collins's calculus with Weingarten functions [44]; see the Supplemental Material [46] A. Equipped with this new representation-theoretic technique, we show in the Supplemental Material [46] C that the deviation of the Clifford group from a unitary 4-design is—in a precise sense—mild enough for the task at hand.

Our final result addresses the *unitarity* of a quantum channel. Introduced by Wallman *et al.* [8], the unitarity is a measure for the coherence of a (noise) channel $\mathcal{E}$. It is defined to be the average purity of the output states of a slightly altered channel $\mathcal{E}'$ [82]

$$u(\mathcal{E}) = \int d\psi \operatorname{Tr}(\mathcal{E}'(|\psi\rangle\langle\psi|)^\dagger \mathcal{E}'(|\psi\rangle\langle\psi|)) \qquad (6)$$

that flags the absence of trace preservation and unitality. The unitarity can be estimated efficiently by using techniques similar to randomized benchmarking [83]. It is also an important figure of merit when one aims to compare the AGF of a noisy gate implementation to its diamond distance [39,40]—a task that is important for certifying fault-tolerance capabilities of quantum devices.

Although useful, the existing definition of the unitarity (6) is arguably not very intuitive. Here, we try to (partially) amend this situation by providing a simple statistical interpretation:

Theorem 3. (Operational interpretation of unitarity) Let $\{\mathcal{U}_k\}_{k=1}^N$ be the gate set of a unitary 2-design. Then, for all Hermiticity-preserving maps $\mathcal{X}$

$$\mathrm{Var}[F_{\rm avg}(\mathcal{U}_k, \mathcal{X})] = \frac{u(\mathcal{X})}{d^2(d+1)^2}, \qquad (7)$$

where the variance is computed with respect to $\mathcal{U}_k$ drawn randomly from the unitary 2-design.

The proof of the theorem is given in the Supplemental Material [46] G. Note that the variance is taken with respect to unitaries drawn from the unitary 2-design and not the variance of the average fidelity with respect to the input state as calculated, e.g., in Ref. [84].

In this Letter, we address the crucial task of characterizing quantum channels. We do so by relying on AGFs of the quantum channel of interest with simple-to-implement Clifford gates. More specifically, we start by noting that (i) the unital part of any quantum channel can be written in terms of a unitary 2-design with expansion coefficients given by AGFs. As a consequence, for certain Hilbert space dimensions d, the unital part can be reconstructed from d^4 AGFs with Clifford-group operations by a straightforward and stable expansion formula. (ii) As the main result, we prove for the case of unitary gates that the reconstruction can be practically done using only essentially order of d^2 random AGFs with Clifford gates. In a simplified measurement setting, we prove that this also leads to a resource optimal scaling in terms of the total number of channel invocations required to estimate the AGFs up to a precision of ε. For the proof, we derive a formula for the integration of fourth moments over the Clifford group, which is similar to Collins's calculus with Weingarten functions. This integration formula might also be useful for other purposes. (iii) We prove that the unitarity of a quantum channel, which is a measure for the coherence of noise [8], has a simple statistical interpretation: It corresponds to the variance of the AGF with unitaries sampled from a unitary 2-design.

The focus of this work is on the reconstruction of quantum gates. Here, the assumption of unitarity considerably simplifies the representation-theoretic effort for establishing the fourth moment bounds required for applying strong existing proof techniques from low-rank matrix recovery. These extend naturally to higher Kraus ranks, and we leave this generalization to future work. Existing results [85,86] indicate that the deviation of the Clifford group from a unitary 4-design may become more pronounced when the rank of the states or channels in question increases. This may lead to a nonoptimal rank scaling of the required number of observations m. In fact, a straightforward extension of Theorem 2 to the Kraus rank-r case already yields a recovery guarantee with a scaling of $m \sim r^5 d^2 \log(d)$.

Practically, it is important to explore how this protocol behaves when applied to data obtained from interleaved randomized benchmarking experiments. Such numerical studies would further allow for a comparison to other established schemes such as GST, for which no theoretical guarantees exist. In Ref. [29], the authors show how to use interleaved randomized benchmarking experiments to measure the AGF between a known Clifford gate and the combined process of an unknown gate concatenated with the average Clifford error process. In order to obtain tomographic information about the isolated unknown gate, the authors had to do a linear inversion of the average Clifford error. However, in most cases, we expect the average Clifford error to be close to a depolarizing channel which has very high rank. Thus, building on our intuition obtained for quantum states [87] and using our techniques, we could obtain a low-rank approximation to the combined unknown gate and average Clifford error, which under the assumption of a high-rank Clifford error, would naturally pick out the coherent part of the unknown gate.

We thank Steven T. Flammia, Christian Krumnow, Robin Harper, and Michał Horodecki for inspiring discussions and helpful comments. R. K. is particularly grateful for a "peaceful disagreement" (we borrow this term from Ref. [88]) with Mateus Araújo that ultimately led to our current understanding of the relation between Clifford gates and tight frames. We used code from Refs. [89–91] to run our simulations. The work of I. R., R. K., and J. E. was funded by analog quantum simulators (AQuS), DFG (Grants No. SPP1798 CoSIP, No. EI 519/9-1, No. EI 519/7-1, and No. EI 519/14-1), the ERC (TAQ), and the Templeton Foundation. The project leading to this application has received funding from the European Union's Horizon 2020 research and innovation programme under Grant agreement No. 817482 (PASQUANS). "Parts of Y. K. L.'s work were carried out in the context of the MURI project 'Optimal Measurements for Scalable Quantum Technologies' funded by the Air Force Office of Scientific Research. Contributions to this work by NIST, an agency of the U.S. Government, are not subject to U.S. copyright. Any mention of commercial products does not indicate endorsement by NIST. D. G.'s work has been supported by the Excellence Initiative of the German Federal and State Governments (ZUK 81), the ARO under Contract No. W911NF-14-1-0098 (Quantum Characterization, Verification, and Validation), Universities Australia and DAAD's Joint Research Co-operation Scheme (using funds provided by the German Federal Ministry of Education and Research), and the DFG (SPP1798 CoSIP, Project No. B01 of CRC 183). The work of M. K. was funded by the National Science Centre, Poland within the project Polonez (Project No. 2015/19/P/ST2/03001), which has received funding from the European Union's Horizon 2020 research and innovation program under the Marie Skłodowska-Curie Grant No. 665778.

*i.roth@fu-berlin.de
†science@mkliesch.eu

[1] J. Emerson, R. Alicki, and K. Życzkowski, Scalable noise estimation with random unitary operators, J. Opt. B 7, S347 (2005).

[2] B. Lévi, C. C. López, J. Emerson, and D. G. Cory, Efficient error characterization in quantum information processing, Phys. Rev. A **75**, 022314 (2007).

[3] 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).

[4] 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).

[5] 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).

[6] E. Magesan, J. M. Gambetta, and J. Emerson, Characterizing quantum gates via randomized benchmarking, Phys. Rev. A **85**, 042311 (2012).

[7] E. Magesan, J. M. Gambetta, and J. Emerson, Scalable and Robust Randomized Benchmarking of Quantum Processes, Phys. Rev. Lett. **106**, 180504 (2011).

[8] J. Wallman, C. Granade, R. Harper, and S. T. Flammia, Estimating the coherence of noise, New J. Phys. **17**, 113020 (2015).

[9] J. J. Wallman, Randomized benchmarking with gate-dependent noise, Quantum **2**, 47 (2018).

[10] J. Helsen, J. J. Wallman, S. T. Flammia, and S. Wehner, Multi-qubit randomized benchmarking using few samples, arXiv:1701.04299.

[11] J. J. Wallman and S. T. Flammia, Randomized benchmarking with confidence, New J. Phys. **16**, 103032 (2014).

[12] R. Blume-Kohout, J. King Gamble, E. Nielsen, J. Mizrahi, J. D. Sterk, and P. Maunz, Robust, self-consistent, closed-form tomography of quantum logic gates on a trapped ion qubit, arXiv:1310.4492.

[13] S. T. Flammia, D. Gross, Y.-K. Liu, and J. Eisert, Quantum tomography via compressed sensing: Error bounds, sample complexity and efficient estimators, New J. Phys. **14**, 095022 (2012).

[14] C. H. Baldwin, A. Kalev, and I. H. Deutsch, Quantum process tomography of unitary and near-unitary maps, Phys. Rev. A **90**, 012110 (2014).

[15] M. Kliesch, R. Kueng, J. Eisert, and D. Gross, Improving compressed sensing with the diamond norm, IEEE Trans. Inf. Theory **62**, 7445 (2016).

[16] M. Kliesch, R. Kueng, J. Eisert, and D. Gross, Guaranteed recovery of quantum processes from few measurements, arXiv:1701.03135.

[17] M. Holzäpfel, T. Baumgratz, M. Cramer, and M. B. Plenio, Scalable reconstruction of unitary processes and Hamiltonians, Phys. Rev. A **91**, 042129 (2015).

[18] D. Gross, Y.-K. Liu, S. T. Flammia, S. Becker, and J. Eisert, Quantum State Tomography via Compressed Sensing, Phys. Rev. Lett. **105**, 150401 (2010).

[19] D. Gross, Recovering low-rank matrices from few coefficients in any basis, IEEE Trans. Inf. Theory **57**, 1548 (2011).

[20] Y.-K. Liu, Universal low-rank matrix recovery from Pauli measurements, Adv. Neural Inf. Process. Syst. **24**, 1638 (2011), https://papers.nips.cc/paper/4222-universal-low-rank-matrix-recovery-from-pauli-measurements.

[21] A. Shabani, R. L. Kosut, M. Mohseni, H. Rabitz, M. A. Broome, M. P. Almeida, A. Fedrizzi, and A. G. White, Efficient Measurement of Quantum Dynamics via Compressive Sensing, Phys. Rev. Lett. **106**, 100401 (2011).

[22] A. Kalev, R. L. Kosut, and I. H. Deutsch, Quantum tomography protocols with positivity are compressed sensing protocols, npj Quantum Inf. **1**, 15018 (2015).

[23] R. Kueng, Low rank matrix recovery from few orthonormal basis measurements, in *Proceedings of the 2015 International Conference on Sampling Theory and Applications (SampTA), Washington, DC, USA 2015*, (IEEE, New York, 2015), pp. 402–406, DOI: 10.1109/SAMPTA.2015.7148921.

[24] M. Kabanava, R. Kueng, H. Rauhut, and U. Terstiege, Stable low-rank matrix recovery via null space properties, Inf. Infer. **5**, 405 (2016).

[25] M. Cramer, M. B. Plenio, S. T. Flammia, R. Somma, D. Gross, S. D. Bartlett, O. Landon-Cardinal, D. Poulin, and Y.-K. Liu, Efficient quantum state tomography, Nat. Commun. **1**, 149 (2010).

[26] B. Lanyon, C. Maier, M. Holzapfel, T. Baumgratz, C. Hempel, P. Jurcevic, I. Dhand, A. Buyskikh, A. Daley, M. Cramer, M. Plenio, R. Blatt, and C. Roos, Efficient tomography of a quantum many-body system, Nat. Phys. **13**, 1158 (2017).

[27] M. P. da Silva, O. Landon-Cardinal, and D. Poulin, Practical Characterization of Quantum Devices without Tomography, Phys. Rev. Lett. **107**, 210404 (2011).

[28] O. Landon-Cardinal and D. Poulin, Practical learning method for multi-scale entangled states, New J. Phys. **14**, 085004 (2012).

[29] S. Kimmel, M. P. da Silva, C. A. Ryan, B. R. Johnson, and T. Ohki, Robust Extraction of Tomographic Information via Randomized Benchmarking, Phys. Rev. X **4**, 011050 (2014).

[30] S. Kimmel and Y. K. Liu, Phase retrieval using unitary 2-designs, in *Proceedings of the 2017 International Conference on Sampling Theory and Applications (SampTA), Tallin, Estonia, 2017*, (IEEE, New York, 2017), pp. 345–349 [arXiv:1510.08887, DOI: 10.1109/SAMPTA.2017.8024414].

[31] R. Barends *et al.*, Rolling quantum dice with a superconducting qubit, Phys. Rev. A **90**, 030303 (2014).

[32] A. Carignan-Dugas, J. J. Wallman, and J. Emerson, Characterizing universal gate sets via dihedral benchmarking, Phys. Rev. A **92**, 060302 (2015).

[33] A. W. Cross, E. Magesan, L. S. Bishop, J. A. Smolin, and J. M. Gambetta, Scalable randomised benchmarking of non-Clifford gates, npj Quantum Inf. **2**, 16012 (2016).

[34] W. G. Brown and B. Eastin, Randomized benchmarking with restricted gate sets, Phys. Rev. A **97**, 062323 (2018).

[35] A. K. Hashagen, S. T. Flammia, D. Gross, and J. J. Wallman, Real randomized benchmarking, Quantum **2**, 85 (2018).

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

[37] S. T. Flammia and Y.-K. Liu, Direct Fidelity Estimation from Few Pauli Measurements, Phys. Rev. Lett. **106**, 230501 (2011).

[38] A. Acin, I. Bloch, H. Buhrman, T. Calarco, C. Eichler, J. Eisert, D. Esteve, N. Gisin, S. J. Glaser, F. Jelezko, S. Kuhr, M. Lewenstein, M. F. Riedel, P. O. Schmidt, R. Thew, A.

Wallraff, I. Walmsley, and F. K. Wilhelm, The European quantum technologies roadmap, New J. Phys. **20**, 080201 (2018).

[39] R. Kueng, D. M. Long, A. C. Doherty, and S. T. Flammia, Comparing Experiments to the Fault-Tolerance Threshold, Phys. Rev. Lett. **117**, 170502 (2016).

[40] J. J. Wallman, Bounding experimental quantum error rates relative to fault-tolerant thresholds, arXiv:1511.00727.

[41] H. Zhu, R. Kueng, M. Grassl, and D. Gross, The Clifford group fails gracefully to be a unitary 4-design, arXiv:1609.08172.

[42] J. Helsen, J. J. Wallman, and S. Wehner, Representations of the multi-qubit Clifford group, J. Math. Phys. (N.Y.) **59**, 072201 (2018).

[43] D. Gross, S. Nezami, and M. Walter, Schur-Weyl duality for the Clifford group with applications, arXiv:1712.08628.

[44] B. Collins, Moments and cumulants of polynomial random variables on unitary groups, the Itzykson-Zuber integral, and free probability, Int. Math. Res. Not. **2003**, 953 (2003).

[45] B. Collins and P. Sniady, Representations of Lie groups and random matrices, Trans. Am. Math. Soc. **361**, 3269 (2009).

[46] See the Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.121.170502, which contains the mathematical details and proofs of the main theorems, an analysis of the optimal number of channel uses, more details on the numerical demonstrations, and further references which include Refs. [47–61].

[47] M. Horodecki, P. Horodecki, and R. Horodecki, General teleportation channel, singlet fraction, and quasidistillation, Phys. Rev. A **60**, 1888 (1999).

[48] M. A. Nielsen, A simple formula for the average gate fidelity of a quantum dynamical operation, Phys. Lett. A **303**, 249 (2002).

[49] R. Goodman and N. R. Wallach, *Symmetry, Representations, and Invariants* (Springer, Berlin, 2009).

[50] W. Fulton and J. Harris, *Representation Theory* (Springer Science & Business Media, New York, 1991), Vol. 129.

[51] E. P. Wigner, *Group Theory and Its Application to the Quantum Mechanics of Atomic Spectra* (Academic Press, London, 1959).

[52] J. A. Tropp, Convex recovery of a structured signal from independent random linear measurements, in *Sampling Theory, a Renaissance*, edited by E. G. Pfander (Springer, New York, 2015), pp. 67–101 [arXiv:1405.1102].

[53] S. Mendelson, Learning without concentration, J. Assoc. Comput. Mach. **62**, 1 (2015).

[54] V. Koltchinskii and S. Mendelson, Bounding the smallest singular value of a random matrix without concentration, Int. Math. Res. Not. **2015**, rnv096 (2015).

[55] J. A. Tropp, User friendly tools for random matrices. An introduction, Defense Technical Information Center, Technical Report No. ADA576100, 2012.

[56] J. Haah, A. W. Harrow, Z. Ji, X. Wu, and N. Yu, Sample-optimal tomography of quantum states, IEEE Trans. Inf. Theory **63**, 5628 (2017).

[57] T. M. Cover and J. A. Thomas, *Elements of Information Theory* (John Wiley & Sons, New York, 2012).

[58] P. Diaconis and M. Shahshahani, On the eigenvalues of random matrices, J. Appl. Probab. **31**, 49 (1994).

[59] R. Vershynin, Introduction to the non-asymptotic analysis of random matrices, in *Compressed Sensing: Theory and Applications* (Cambridge University Press, Cambridge, England, 2012), pp. 210–268.

[60] S. Foucart and H. Rauhut, *A Mathematical Introduction to Compressive Sensing* (Springer, New York, 2013).

[61] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, Quantum error correction via codes over GF(4), IEEE Trans. Inf. Theory **44**, 1369 (1998).

[62] C. B. Mendl and M. M. Wolf, Unital quantum channels—Convex structure and revivals of Birkhoff's theorem, Commun. Math. Phys. **289**, 1057 (2009).

[63] D. Gross, K. Audenaert, and J. Eisert, Evenly distributed unitaries: On the structure of unitary designs, J. Math. Phys. (N.Y.) **48**, 052104 (2007).

[64] P. Delsarte, J. Goethals, and J. Seidel, Spherical codes and designs, Geometriae Dedicata **6**, 363 (1977).

[65] J. M. Renes, R. Blume-Kohout, A. J. Scott, and C. M. Caves, Symmetric informationally complete quantum measurements, J. Math. Phys. (N.Y.) **45**, 2171 (2004).

[66] H. Zhu, Multiqubit Clifford groups are unitary 3-designs, Phys. Rev. A **96**, 062336 (2017).

[67] Z. Webb, The Clifford group forms a unitary 3-design, Quantum Inf. Comput. **16**, 1379 (2016), http://www.rintonpress.com/journals/qiconline.html#v16n1516.

[68] R. Kueng and D. Gross, Qubit stabilizer states are complex projective 3-designs, arXiv:1510.02767.

[69] A. J. Scott, Tight informationally complete quantum measurements, J. Phys. A **39**, 13507 (2006).

[70] D. M. Appleby, Symmetric informationally complete-positive operator valued measures and the extended Clifford group, J. Math. Phys. (N.Y.) **46**, 052107 (2005).

[71] D. Gross, F. Krahmer, and R. Kueng, A partial derandomization of PhaseLift using spherical designs, J. Fourier Anal. Appl. **21**, 229 (2015).

[72] A. J. Scott, Optimizing quantum process tomography with unitary 2-designs, J. Phys. A **41**, 055308 (2008).

[73] H. F. Chau, Unconditionally secure key distribution in higher dimensions by depolarization, IEEE Trans. Inf. Theory **51**, 1451 (2005).

[74] A. Ambainis, J. Bouda, and A. Winter, Nonmalleable encryption of quantum information, J. Math. Phys. (N.Y.) **50**, 042106 (2009).

[75] M. Fazel, H. Hindi, and S. Boyd, A rank minimization heuristic with application to minimum order system approximation, Proc. Am. Control Conf., **6**, 4734 (2001).

[76] I. Roth, R. Kueng, S. Kimmel, Y.-K. Liu, D. Gross, J. Eisert, and M. Kliesch, Quantum process tomography with average gate fidelities, GitHub repository (2017), https://github.com/MartKl/Quantum_process_tomography_with_average_gate_fidelities.

[77] E. J. Candès, T. Strohmer, and V. Voroninski, PhaseLift: Exact and stable signal recovery from magnitude measurements via convex programming, Commun. Pure Appl. Math. **66**, 1241 (2013).

[78] E. Candès and X. Li, Solving quadratic equations via PhaseLift when there are about as many equations as unknowns, Found. Comput. Math. **14**, 1017 (2014).

[79] R. Kueng, H. Rauhut, and U. Terstiege, Low rank matrix recovery from rank one measurements, Appl. Comput. Harmon. Anal. **42**, 88 (2017).

[80] F. Krahmer and Y. K. Liu, Phase retrieval without small-ball probability assumptions, IEEE Trans. Inf. Theory **64**, 485 (2018).

[81] The cardinality of the Clifford group grows superpolynomially in the Hilbert space dimension d. Therefore, the nonspikiness with respect to the Clifford group quickly corresponds to a demanding number of constraints. In fact, about 10^8 and 10^{13} constraints are already required for 3-qubits and 4-qubits, respectively.

[82] $\mathcal{E}'$ is defined so that $\mathcal{E}'(Id) = 0$ and $\mathcal{E}'(X) = \mathcal{E}(X) - \mathrm{Tr}[\mathcal{E}(X)]/\sqrt{d}Id$ for all traceless X.

[83] G. Feng, J. J. Wallman, B. Buonacorsi, F. H. Cho, D. K. Park, T. Xin, D. Lu, J. Baugh, and R. Laflamme, Estimating the Coherence of Noise in Quantum Control of a Solid-State Qubit, Phys. Rev. Lett. **117**, 260501 (2016).

[84] E. Magesan, R. Blume-Kohout, and J. Emerson, Gate fidelity fluctuations and quantum process invariants, Phys. Rev. A **84**, 012309 (2011).

[85] R. Kueng, H. Zhu, and D. Gross, Low rank matrix recovery from Clifford orbits, arXiv:1610.08070.

[86] R. Kueng, H. Zhu, and D. Gross, Distinguishing quantum states using Clifford orbits, arXiv:1609.08595.

[87] C. A. Riofrio, D. Gross, S. T. Flammia, T. Monz, D. Nigg, R. Blatt, and J. Eisert, Experimental quantum compressed sensing for a seven-qubit system, Nat. Commun. **8**, 15305 (2017).

[88] M. Araújo, More Quantum (2016), http://mateusaraujo.info/2016/08/02/understanding-bells-theorem-part-3-the-many-worlds-version/.

[89] N. Johnston, QETLAB: A MATLAB toolbox for quantum entanglement, version 0.9, 2016, http://qetlab.com.

[90] E. Magesan, A Random Clifford sampler for MATLAB, (private communication with S.K.,2011).

[91] M. P. da Silva, QIP MATLAB Library, 2012, https://github.com/marcusps/QIP.m.