Randomized benchmarking for individual quantum gates

E. Onorati, A. H. Werner, and J. Eisert

1Dahlem Center for Complex Quantum Systems, Freie Universität Berlin, 14195 Berlin, Germany
2Department of Mathematical Sciences, University of Copenhagen, DK-2100 København, Denmark
3Department of Mathematics and Computer Science, Freie Universität Berlin, 14195 Berlin, Germany

Any technology requires precise benchmarking of its components, and the quantum technologies are no exception. Randomized benchmarking allows for the relatively resource economical estimation of the average gate fidelity of quantum gates from the Clifford group, assuming identical noise levels for all gates, making use of suitable sequences of randomly chosen gates. In this work, we report significant progress on randomized benchmarking, by showing that it can be applied individually on a broad class of quantum gates outside the Clifford group, even for varying noise levels per quantum gate. This is possible at little overhead of quantum resources, but at the expense of a significant classical computational cost. At the heart of our analysis is a representation-theoretic framework which we bring into contact with classical estimation techniques based on bootstrapping and matrix pencils. We demonstrate the functioning of the scheme at hand of benchmarking tensor powers of $T$-gates. Apart from its practical relevance, we expect this insight to be relevant as it highlights the role of assumptions made on unknown noise processes when characterizing quantum gates at high precision.

Recent years have seen a rapid development in the precise preparation and manipulation of quantum states. Much of these advances have been triggered by the progress in the quantum technologies, anticipating computational quantum devices that outperform classical computers [1]. The increased sophistication of these experiments, however, is accompanied by an increased complexity of the task of verifying that the process has actually been implemented as expected. Unwanted and usually largely uncharacterized quantum noise hampers the correct functioning of quantum devices. Without the knowledge of such noise processes, yet, it is unclear how to achieve actionable advice on how to improve the experiment or whether the experiment has worked at all. The task of certifying quantum processes has hence been identified, unsurprisingly, as a key bottleneck in the field.

There are several strategies that can in principle be employed to tackle the problem. They can largely be classified in the assumptions they make about the given unknown process and the structure they employ. Quantum process tomography [2,3] is an option, in principle, in that based on measurement data alone, an unknown process can be reconstructed. However, without any further structure or assumptions the scaling of the effort of quantum process tomography is daunting: for a generic $d$-dimensional quantum system, $\Theta(d^4)$ expectation values must be estimated to great accuracy. Methods exploiting structure, such as process tomography based on compressed sensing [4,5] or diamond norm minimization [6] reduce the effort significantly. Also, the dynamics of quantum systems for short times can often be kept track of using tensor network states [7,8]. Nevertheless, the benchmarking of large quantum circuits involving a large number of gates is out of scope in either of these approaches. This challenge is aggravated by the fact that gate errors suitable for fault tolerant quantum computing [1,9,11] are extremely small, so that the characterization needs to be very precise.

Randomized benchmarking [12–18] – introduced in Ref. [12] – takes a different, more pragmatic route altogether. It acknowledges that full tomographic knowledge may be too much to ask for and achieves estimates of quantum gate errors making use of long sequences of randomly chosen Clifford gates. This is done to estimate a single quantity, the average gate fidelity, for a set of operations being the Clifford group in a large portion of the literature. That is to say, by making stronger assumptions about the underlying operations, one can go a long way reliably characterizing noise levels of quantum gates. The basic idea has been generalised in several ways; in particular, it has been shown that one does not need to employ an exact so-called 2-design for randomized benchmarking [13,19,20], using instead, for instance, the single-qubit dihedral group [21]. To allow for extraction of the fidelity of a specific gate, a scheme called interleaved randomized benchmarking [22,23] makes use of random sequences of Clifford gates interleaved by the particular gate whose noise is to be individually characterized, but it is still limited to the Clifford group itself or the $T$-gate. For protocols based on twirls over 2-design gates sets, such as the Clifford group, it has been recently shown [23] that they allow for strongly gate-dependent noise levels. However, other schemes which are able to go beyond the 2-design requirement assume the noise to be gate-independent [25], or weakly dependent [26]. In several ways the commonly made assumptions on the underlying processes are rather strong. For protocols not relying on 2-designs property, the premise on uniform noise channel for each gate of the group may be overly demanding; even if we take into consideration small generating gates sets, it is difficult to postulate that the noise of a single gate is equal to the one of a product of several consecutive operators. Here, we will see that some of these assumptions can be relaxed at little additional cost, as far as quantum resources are concerned.

In this work, we introduce the notion of randomized benchmarking for individual quantum gates, one that may be part of single layers of gate arrays. This work is expected to be significant in two ways: technically speaking, we introduce methods able to benchmark quantum gates individually, including ones that are outside the Clifford group. Since schemes for universal quantum computing necessarily make use of such
gates, this seems an important step forward. At the same time, we do not require twirling over the full Clifford group or a 2-design, but only over a relatively small local symmetry group coupled with transpositions gates. It is indeed a favourable feature of our approach to make use of a small group in contrast to large gate sets of previously known schemes.

The novel idea in the present work is to exploit the symmetry of the quantum gate itself in an appropriate fashion and hence reduce the amount of quantum resources and computational effort. To achieve this goal, we harness advanced tools from representation theory to arrive at schemes that require similar physical operations, departing from the paradigm of 2-designs, but which can make predictions beyond known prescriptions. These ideas are uplifted to functioning schemes by making use of estimation techniques such as matrix pencils [27]. It is key to the new approach that the demands for classical estimation are higher, which we accommodate by introducing more sophisticated tools to this task. Using such methods, we demonstrate that meaningful and experimentally accessible preparations are sufficient to render the recovery feasible at hand of randomized benchmarking data.

More conceptually speaking, and putting this contribution into a broader context, we show that one can interpolate between common assumptions made when characterizing quantum processes: In other words, there is “room in the middle” between full quantum process tomography, which is largely assumption-free but comes along with daunting resource requirements, and conventional randomized benchmarking, which requires significantly less effort and is also robust against state preparation and measurement (SPAM) errors, while making strong assumptions. Complementing this mindset in a very different way, Refs. [5, 28] provide method to extract tomographic information making use standard randomized benchmarking protocols, while maintaining very large data levels. We believe that this conceptual insight into the ontology of assumptions when characterizing quantum processes subject to quantum noise is equally important.

Exploiting local symmetries in randomized benchmarking. In the following, we are going to describe a protocol that provides the average gate fidelity of the noisy channel Λ which characterizes the imperfect implementation ˜U of a target ideal unitary gate U,

$$\mathbb{E}(\mathcal{F}_{\tilde{U},U}) = \mathbb{E}(\mathcal{F}_{\Lambda,U}) := \int_{\text{Haar}} \text{Tr} [\langle \phi | \Lambda(|\phi\rangle \langle \phi|)] \, d\phi. \tag{1}$$

It is key to our method to explicitly exploit the local and permutation symmetries of U, allowing for a drastic reduction of the fitting parameters, and also to inherit robustness with respect to SPAM errors. In this way, fitting models of well-known randomized benchmarking protocols can be uplifted to this setting involving fewer assumptions.

Throughout this work, we consider quantum gates acting on n-qubit systems and we are interested in benchmarking the accuracy of their implementation in a quantum circuit making use of the protocol that we are going to explain in a later section. The method is particularly suitable for gates consisting of tensor products of local gates, thus admitting additional symmetries with respect to the exchange of qubit subsystems and hence it is applicable in those situations of single layers of local unitary quantum gates. For concreteness, we shall put emphasis on single layers of circuits whose gates consist of tensor compositions of the T-gate with other gates belonging to the Clifford group C_n, namely H, S and CNOT

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad T = \begin{pmatrix} e^{-i\pi/8} & 0 \\ 0 & e^{i\pi/8} \end{pmatrix}, \quad \text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \tag{2}$$

leading to a universal set. This setting is of paramount importance in state-of-the-art prescriptions of fault-tolerant quantum computing [11]. More generally, the protocol is suitable to benchmark tensor products of local gates consisting in arbitrary rotations around one of the axes of the Bloch sphere. We will denote with $U = U_1 \otimes \cdots \otimes U_m$ the multi-qubit unitary operator – with U_j one or two qubits each – that we intend to benchmark, acting as a single layer of a unitary circuit. At the heart of the analysis will be its symmetry group, constructed from the symmetries of the local gates $U_j$ composing U and the permutations of qubits which the local gate acts upon (cf. Appendix D). More precisely, we choose the local symmetry group $A_j$ of $U_j$ as the subset of the single-qubit Clifford group, $C_1$, whose elements commute with $U_j$. E.g., for $U_j = T = \exp(-i\pi Z/8)$, the group of local symmetries is

$$A_T := \{ U \in C_1 : U^\dagger Z U = Z \}.$$

This is an abelian group of 4 elements isomorphic to the cyclic group of order 4, $Z_4$. The set of all possible permutations interchanging qubits affected by the same local gate is another symmetry group of the target unitary $U_j$; taking a practical example, for the gate $U = T \otimes H \otimes T \otimes H \otimes T$, this group is isomorphic to $S_3 \times S_2$, i.e., all permutations of the first, third and fifth subsystems combined with the transposition of the second and forth subsystems. The full symmetry group $G$ is then obtained through the semi-direct product $A_n \rtimes \Pi$, where $A_n$ is the direct product of the local symmetry groups $A_j$ constructed by the Kronecker product of the respective elements, and $\Pi$ is the representation of the subgroup of $S_n$ consisting of all allowed permutations of the qubits subsystems.

Role of abelian groups. In order to apply our full protocol and combine the group $A_n$ with $\Pi$, all local symmetry groups $A_j$ must be abelian. This is indeed a necessary condition to reconstruct the irreducible representations of the full group $G$ with the sole knowledge of the composing groups, as we will discuss in the appendix [29]. Fortunately, this is the case for the centralizer in $C_1$ of the gates in Eq. (2) and all other rotations around one of the Bloch axes. Should the local symmetry groups not be all abelian, the protocol is still valid setting $G = A_n$, i.e., without considering permutation symmetries.

Assumptions and physical motivation. We denote with calligraphic letters the channel acting by gate conjugation on density operators, i.e., $\mathcal{U}(\rho) := U^\dagger \rho U$ and the noisy implementation of the idealized gate channel $\mathcal{U}$ as $\tilde{\mathcal{U}} := \Lambda \circ \mathcal{U}$,
i.e., we account for a gate-dependent error channel $\Lambda_U$ whose average fidelity we want to characterize with the proposed protocol. As randomized benchmarking can be interpreted as a trade-off between the level of characterization of the noise channel and the amount of physical and computational resources needed, we will make the following assumption: the Pauli-Liouville representation (cfr. Appendix E) of the twirled noise channel, $\Lambda_U^G := |G|^{-1} \sum_{j \in G} g_j^* \Lambda_U g_j$, is almost jointly diagonalizable with the target unitary channel $U$ (where again we consider it as a matrix in Pauli-Liouville representation), in the spirit of Ref. [30]. This means that when the matrix $U$ is brought to diagonal form by some unitary transformation $V$, the off-diagonal element of $\Lambda_U^G$ under the same transformation are small and in particular, $\Lambda_U^G$ will approximately leave the same subspaces invariant. This is true in two cases. The first possibility is that both $U$ and the twirled noise $\Lambda_U^G$ are diagonalizable simultaneously in a certain basis, e.g., when the decomposition of the representation of the symmetry group into irreducible representations has no multiplicity: in this case, both $U$ and the twirled noise $\Lambda_U^G$ are “forced” to assume a diagonal form with respect to the irreducible subspaces. If this is not the case, then $\Lambda_U^G$ assumes a sparse form with some off-diagonal entries, which have to be small with respect to the diagonal elements. This is fulfilled whenever the original noise channel $\Lambda_U$ related to the implementation of the gate $U$ was almost jointly diagonalizable to begin with or, put in another perspective [30], it is almost commuting. This assumption is valid when the gate $U$ is generated by a Hamiltonian $H$ applied for some run time $t$ [31], i.e., $U = e^{-iHT}$, which can be perturbed for a small fraction of the time, or be applied for too much or too little time (please refer to Section F in the appendix for more details). Furthermore, we ask the gates belonging to the symmetry group $G$ to be implementable with high accuracy (see Appendix I). These gates either perform a permutation of the subspaces of the system or belong to the Clifford group and so can be for instance benchmarked with the well-known methods [13][16][24].

The protocol. We propose a slightly modified version of the previous protocols. We apply in succession channels defined by the gate $U$ after the one induced by a gate uniformly drawn at random from the symmetry group $G$. In addition, we can target the different symmetry subspaces that are stabilized by $G$ by choosing an appropriate initial state through the application of projectors decomposing a density operator into basis vectors of distinct irreducible subspaces (see Ref. [32] and Appendix L, Section 2). Note that, unlike previous protocols, the target gate $U$ is not part of the twirling group $G$. This is one of the reason why one can benchmark arbitrarily small rotations over the Bloch axes with a relatively small number of gates. For a fixed sequence length $\ell$ the protocol consists of the steps:

(i) Prepare an initial state $\rho$ with support in the target invariant subspace(s).

(ii) Draw a random sequence $k_\ell = (k_1, \ldots, k_\ell) \in \mathbb{N}_n^\ell$.

(iii) Apply the following operation generated by the symmetry operations $G_{k_j}$ to the initial state $\rho$:

$$C_{k_\ell}(\rho) = G_{k_\ell} \circ U \circ G_{k_{\ell-1}} \circ \cdots \circ U \circ G_{k_2} \circ U \circ G_{k_1},$$

where $G_{k_j} := G_{k_j}^1 \circ \cdots \circ G_{k_j}^n$ is the channel given by the composition of the inversion of all previous random gates channels.

(iv) Perform a suitable POVM $E$, e.g., by applying the projector used to construct the input state $\rho$ according to Eq. (21) in the appendix, and measure the survival probability $F_{k_\ell} = \text{Tr}[E \ C_{k_\ell}(\rho)]$. To obtain an appropriate precision for $F_{k_\ell}$, this step has to be repeated sufficiently often.

(v) Repeat the previous step for sufficiently many (say $N$) random sequences $k_{\ell,1}, \ldots, k_{\ell,N}$ of length $\ell$. Then, calculate the sequences survival probability

$$F_{\text{seq}}(\ell, \rho) = \frac{1}{N} \sum_{k_\ell} F_{k_\ell} = \frac{1}{N} \sum_{k_\ell} \text{Tr}[E \ C_{k_\ell}(\rho)].$$

The number $N$ of random sequences should be chosen such that

$$F_{\text{seq}} \approx F_{\text{avg}},$$

where $F_{\text{avg}}$ is the survival probability averaged over all possible sequences. The choice can be motivated by an analysis on the variance of the random variable $F$, with $F_{k_\ell}$ being a realization and $F_{\text{avg}}$ the mean of the distribution (see Appendix J for a bound on the number of samples). Note that, for a Clifford circuit, one requires a “relatively small” number of sequences to approximate $F_{\text{avg}}$.17][33].

(vi) Repeat the previous steps for different lengths $\ell$.

(vii) Insert $F_{\text{seq}}$ into the zeroth-order fitting model (whose derivation is discussed in the next paragraph),

$$F^{(0)}_{\text{avg}}(\ell, \rho) = \sum_j (\lambda_j d_j) \xi_j$$

where the sum runs over the eigenvalues $\{d_j\}$ of the target matrix $U$ belonging to the space which $\rho$ has support over, with $\xi_j := \text{Tr}[E \Lambda(\{v_j\})(\rho, v_j)]$ absorbing the gate preparation and measurement errors and where $\{v_j\}$ is the set of the basis vectors diagonalizing $U$. The set $\{\lambda_j\}$ corresponds to the diagonal elements of $\Lambda$ with respect to this basis.

(viii) Subsequently, we retrieve the parameters $\{\lambda_j\}$, which characterize the average gate fidelity of $U$ with respect to $U$ (cfr. Appendix H) according to the relation

$$\mathbb{E}(F_{\Lambda(\{\lambda_j\})}) = \frac{\sum j \lambda_j + d}{d(d+1)},$$

using classical estimation techniques.

The fitting model. Considering a noise channel $\Lambda$ (we now drop the subscript $U$ to lighten notation) at each implementation of $U \circ G_{k_\ell}$, we can write

$$C_{k_\ell} = \Lambda' \circ G_{\text{inv}} \circ \cdots \circ U \circ G_k,$$

where the error channel $\Lambda'$ characterizing the implementation of $G_{\text{inv}}$ can be different from the error for the implementation of $U \circ G_{k_\ell}$. Now, defining recursively $B_{k_\ell} := G_{k_\ell} \circ B_{k_{\ell-1}}$
with $B_{k_i} = \mathcal{G}_{k_i}$, and using the invariance of $U$ under the action of $G$, we can rewrite

$$C_{k_i} = N \sum_{\ell=1}^{\ell_{\text{max}}} B_{k_i}^{\dagger} \circ \Lambda \circ B_{k_i} \circ \mathcal{U}. \quad (10)$$

When averaging over all possible sequences, we get $F_{\text{avg}}(\rho) = \text{Tr}[E C_{\text{avg}}(\rho)]$ with $C_{\text{avg}} = N \sum_{\ell=1}^{\ell_{\text{max}}} \Lambda^G \circ \mathcal{U}$, where $\Lambda^G := |G|^{-1} \sum_{j \in G} B_j^{\dagger} \circ \Lambda \circ B_j$ is now like $U$ invariant with respect to the action of $G$. At this point we know that by Schur's Lemma (see Appendix C) the Pauli-Liouville variant with respect to the action of $G$, which brings both into a diagonal form and so, when diagonalizing $\mathcal{U}$, the matrix representation of $\Lambda^G$ will assume a block form, where each of these blocks corresponds to an irreducible representation. For the zeroth-order model, we consider the diagonal elements of $\Lambda^G$ only, and in particular the set $\{ \lambda_j \}$ accounted in Eq. (7) denotes the ones belonging to the support of $\rho$. Let us write $\Lambda^G = \Lambda_0 + \Lambda_{\text{off}}$, with $\Lambda_0$ being jointly diagonalizable with $\mathcal{U}$ and $\Lambda_{\text{off}}$ having smaller matrix entries due to the previously discussed assumption. Then, in zeroth-order, we have $F_{\text{avg}}^{(0)}(\rho) = \text{Tr}[E N \left( \sum_{j=1}^{\ell_{\text{max}}} \Lambda_0 \circ \mathcal{U} \right)(\rho)]$, from which Eq. (7) follows. If one needs to take into consideration off-diagonal entries of $\Lambda^G$ too, a first-order model is necessary (see Appendix G).

Statistical analysis and bootstrapping. In order to estimate the average fidelity with the help of Eq. (9) we need to extract the decay rates $\{ \lambda_j \}$ from the measured data. According to the protocol, this data consists of the survival probabilities $\{ F_{k_{\ell,q}} \}$ measured for $q = 1, \ldots, N$ randomly chosen sequences of lengths $\ell = 1, \ldots, \ell_{\text{max}}$. Let us denote by $F_{\text{seq}}(\ell)$ the average of $F_{k_{\ell,q}}$ with respect to the randomly chosen symmetry-group sequences $k_{\ell,q}$ for fixed sequence length $\ell$. The zeroth-order fitting model from Eq. (7) then tells us that $F_{\text{seq}}(\ell) \approx \sum_j (\lambda_j d_j)^\ell \xi_j$ and accordingly, we can extract the parameters $\{ \lambda_j \}$ from the sequence $(F_{\text{seq}}(\ell))_{\ell=1}^{\ell_{\text{max}}}$ with the help of matrix pencil based signal reconstruction (see Appendix L). In order to improve our estimates we combine this approach with a bootstrapping procedure in the following way: To obtain a single bootstrap sample, we choose from the complete set of measured survival probabilities $\{ F_{k_{\ell,q}} \}_{\ell=1}^{\ell_{\text{max}}}$ for each sequence length $\ell$ a random subset of the sequences $k_{\ell,q}$ for which we then compute the average $F_{\text{seq}}^{\text{boot}}(\ell)$ and extract $\{ \lambda_j \}$ as described before. Repeating this process for different random samples of the $k_{\ell,q}$, we obtain different estimates for the average fidelity, which is then averaged again with respect to the bootstrap samples in order to produce our final estimate for the average fidelity.

Recovery for single $T$-gate and two $T$-gates. In order to check the performance of our proposed protocol, we consider two examples: A single $T$-gate and the tensor product of two $T$-gates. In the single $T$-gate case, the generating Hamiltonian is perturbed by an additional $\sigma_x$ term and we write $H = \frac{\pi}{8} \sigma_z - \varepsilon \sigma_x$, whereas in the two $T$-gates we consider $H = \frac{\pi}{4} (\sigma_z \otimes \mathbb{1} + \mathbb{1} \otimes \sigma_z - \varepsilon \sigma_x \otimes \sigma_x)$ for varying perturbation strength $\varepsilon$.

Figure 1. Average fidelity for noisy single $T$-gate (a) and two $T$-gates (b) for different noise-strengths $\varepsilon$ extracted from bootstrapping over $N = 100$ sequences of length up to $\ell = 1000$ (a) and $\ell = 1600$ (b). Green lines and stars indicate the analytic value of the average fidelity $\mathbb{E}(\mathcal{F})$ for the given noise level, whereas red diamonds the fitted average fidelity for the zeroth-order model.

Conclusions and outlook. In this work, we have proposed a novel approach to randomized benchmarking, developing a protocol that allows to estimate individually the average gate fidelity of a unitary operator whose imperfect implementation is described by a gate-dependent noise channel, hence lifting some of the weaknesses related to the well-known protocols while maintaining robustness against SPAM errors. The key idea involves the twirl of the noise channel over the symmetry group of the target gate given by the composition of local symmetries with respect to the qubit subsystems and permutations thereof: This reduces considerably the amount of parameters that one has to retrieve and also the number of random gates needed. We have produced numerical simulations showing the validity of the protocol for a single-qubit and two-qubit $T$-gate, which proves to be faithful for relatively large noise levels. While we do not have a theoretical formula for the scalability of the protocol, also due to the very wide range of possible gates that can be benchmarked in this way, the example of multiple tensor copies of the $T$-gate in Appendix K suggests that the number of non-linear parameters in the fitting model is drastically inferior compared to the full matrix dimension when increasing the number of qubits. Further investigations in this direction would be certainly of interest. Another open question concerns the number of different random samples needed to approximate the average fidelity with confidence, and in particular to obtain a bound in the fashion of Ref. [34]. With this letter, we hope to further stimulate research on randomized benchmarking outside the more established domain of the Clifford group and to explore the territory between randomized benchmarking and more traditional quantum process tomography.

Acknowledgements. We thank R. Kueng, O. Buerschaper, R. Di Candia, S. T. Flammia, and M. Wageringel for valuable discussions. This work has been supported by the ERC (TAQ), the DFG (El 519/7-1, El 519/11-1, CRC 183, DAEDALUS), the excellence cluster MATH+, and the Templeton Foundation. This work has also received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No. 817482 (PASQuanS). AHW thanks the Humboldt Foundation for its support with a Feodor Lynen Fellowship.


[29] The supplements cite Refs. [15, 17, 27, 28, 33–43].


[38] D. P. O’Leary and B. W. Rust. Variable projection for nonlinear least squares problems. Computational Optimization and
Supplemental material: Randomized benchmarking for individual quantum gates

E. Onorati, A. H. Werner, and J. Eisert
1Dahlem Center for Complex Quantum Systems, Freie Universität Berlin, 14195 Berlin, Germany
2Department of Mathematical Sciences, University of Copenhagen, DK-2100 København, Denmark
3Department of Mathematics and Computer Science, Freie Universität Berlin, 14195 Berlin, Germany

Structure of the appendix

This appendix contains technical details for the scheme proposed in the letter and is structured as follows in order to have some logical flow and help readability. The first Sections A and B provide the basic theoretic elements for group and representation theory, whose most relevant tool to this work is separately given in Section C. As we mentioned in the main part of the letter, the core idea of our novel randomized benchmarking protocol is the coupling of local and permutation symmetries in order to produce a larger symmetry group of the target gate; the machinery for retrieving the irreducible characters of a semi-direct product group from the sole knowledge of the irreducible representations of its constituent subgroups is illustrated in Section D. After this first part, we focus on other particular aspects of the protocol. We justify in Section F the assumption on almost jointly diagonalizable matrix representations of the noise and ideal unitary channels, we discuss in Section G the derivation of a first-order fitting model to account for off-diagonal terms, in Section H we connect the retrieved parameters to the average gate fidelity, we describe how to separate this quantity for the target gate from that, for all $g \in G$, $e \cdot g = g \cdot e = g$.

Inverse: for every element $g \in G$ there exist an inverse element $g^{-1}$ such that $g^{-1} \cdot g = g \cdot g^{-1} = e$.

If two groups can be linked by a group isomorphism, they are said to be *isomorphic*. They will then have many properties in common, in particular the same multiplication table and character table. One can therefore easily obtain information about a group if it is possible to find a group isomorphism connecting it to another well-known group; this is indeed what we do in our protocol to deal with the local symmetry groups. A subset $H \subset G$ is called *subgroup* if all above conditions are still satisfied, e.g., the subset is closed with respect to the group operation. A subgroup $N$ such that $g^{-1} \cdot n \cdot g \in N$ for all $n \in N$, $g \in G$ is said to be *normal* and this is denoted by $N \triangleleft G$.

One can define a (left) group action of $G$ on a set $M$ by a function

$$
\phi : G \times M \to M,
(g,m) \mapsto \phi(g,m)
$$

that fulfills the following two axioms:

*Identity*; for all $m \in M$, $\phi(e,m) = m$.

*Compatibility*; for all $m \in M$, $g,h \in G$ $\phi(g,\phi(h,m)) = \phi(g \cdot h ,m)$. With this definition, we can furthermore define the following.

**Definition 2 (Orbit).** An orbit $G.m$ of an element $m \in M$ is given by all elements in $M$ obtained by the action of $G$, i.e.,

$$
G.m := \{ \phi(g,m) : g \in G \} .
$$

The action of $G$ on $M$ induces a *partition* of the set $M$ itself, i.e., it regroups the elements into subsets such that every element $m \in M$ is contained in one and only one of these.

**Definition 3 (Stabilizer subgroup).** The stabilizer subgroup of $G$ with respect to $m$ is the set of all elements on $G$ such that

$$
G_m := \{ g \in G : \phi(g,m) = m \} .
$$

It is always possible to couple two groups to generate a new one. This is indeed what we are seeking, having to combine symmetry of the local gates together with the invariance with respect to (certain) permutations thereof.

**Definition 4 (Direct product).** Given two groups $G$ and $H$, the direct product $G \times H$ is a Cartesian product of ordered pairs $(g,h)$, with $g \in G$, $h \in H$ equipped with a binary operation acting component-wise, that is

$$(g_1,h_1) \cdot (g_2,h_2) = (g_1 \cdot g_2, h_1 \cdot h_2).$$
This new structure satisfies all axioms of closure, associativity, existence of identity — given by \((e_G, e_H)\) — and inverse element— \((g^{-1}, h^{-1})\) being the inverse of \((g, h)\) — and so it is a group. An alternative way to construct a new group from is given by the semi-direct product.

**Definition 5** (Outer semi-direct product). Let \(N, H\) be groups, \(\varphi : H \to \text{Aut}(N)\) be a homomorphism from \(H\) to the set of automorphisms of \(N\). Then the (outer) semi-direct product with respect to \(\varphi\), denoted by \(G = N \rtimes \varphi H\), is the group whose underlying set are the pairs \((n, h)\in N \times H\) equipped with an operation defined as

\[
\bullet : G \times G \to G \\
((n_1, h_1), (n_2, h_2)) \mapsto (n_1, h_1) \bullet (n_2, h_2) = (n_1 \cdot \varphi_{h_1}(n_2), h_1 \cdot h_2),
\]

where \(n_1, n_2 \in N, h_1, h_2 \in H\).

This structure is again a group according to the defining axioms, with identity element \((e_N, e_H)\) and inverse \((n, h)^{-1} = (\varphi_{h^{-1}}(n^{-1}), h^{-1})\). Note that the the set \(\{(n, e_H) : n \in N\}\) is a normal subgroup of \(G\) isomorphic to \(N\).

It is also possible to go the other way around and obtain from a group \(G\) and a normal subgroup \(N\) a new group called quotient group, denoted by \(G/N\). This is the set of all cosets of \(N\) in \(G\), i.e.,

\[
G/N := \{ gN : g \in G \},
\]

where \(gN\) is the left coset of \(N\) in \(G\), namely

\[
gN := \{ gn : n \in N \}.
\]

The latter definitions stands for all subgroup \(N\), not necessarily normal, however when \(N\) is normal the left coset and the right coset (defined analogously) coincide. The set \(G/N\) is then a group under the operation \((gN) \cdot (hN) = (gh)N\).

We conclude this paragraph with the following definition of the canonical projection which is involved in the construction of irreducible representations of a semi-direct product group, as we will see in the next subsection.

**Definition 6** (Canonical projection). Let \(N \triangleleft G\). The group homomorphism

\[
\tau : G \to G/N, \\
g \mapsto gN
\]

is called canonical projection.

**B. Representation theory**

We are now going to introduce representations and some of the most important results involving them. The following propositions are the mathematical tools at the heart of our randomized benchmarking protocol.

**Definition 7** (Representation). A representation of a group \(G\) on a vector space \(V\) is a group homomorphism onto the general linear group on \(V\), i.e., a map

\[
\pi : H \to GL(V), \\
g \mapsto \pi(g)
\]

such that

\[
\pi(g) \cdot \pi(h) = \pi(g \cdot h).
\]

A representation is said to be faithful if it is injective, and its dimension corresponds to the dimension of the vector field \(V\). A subspace \(W \subset V\) is said to be invariant if, for all \(g \in G\) and \(w \in W\),

\[
\pi(g)w \in W.
\]

Furthermore, a representation is said to be irreducible if the only invariant subspaces are \(\{0\}\) and \(V\) itself; often, this is abbreviated as irrep. Every complex representation of a finite group is completely reducible, i.e., it can be decomposed as a direct sum of irreducible representations. This property, together with Schur’s Lemma, makes irreducible representations and their characters a central object in the theory and will also be particularly relevant in our work.

**Definition 8** (Character of a representation). The character \(\chi_\pi\) of a representation \(\pi\) of a group \(G\) on \(V\) is given by

\[
\chi_\pi(g) = \text{Tr}[\pi(g)].
\]

The dimension of a representation corresponds then to its character at the identity element, \(\chi_\pi(e)\). For finite group, the number of irreducible representations is again finite, and the following result is useful to check if all irreducible representations of a given group have been found.

**Proposition 9** (Group order and irreducible representations dimension). The order of a group \(G\) and the dimension of its irreducible representations are linked by

\[
|G| = \sum_{\alpha : \pi_\alpha \text{irrep}} \chi_{\pi_\alpha}(e)^2.
\]

One of the most important properties for character of irreducible representations is the following orthogonality relation.

**Proposition 10** (Orthogonality formula). Let \(\{\chi_\alpha\}_\alpha\) be the set of characters of all irreducible representations of a group \(G\). Then

\[
\frac{1}{|G|} \sum_{g \in G} (\chi_\alpha(g))^* \chi_\beta(g) = \begin{cases} 1 & \text{if } \alpha = \beta, \\ 0 & \text{if } \alpha \neq \beta. \end{cases}
\]
**Proposition 11** (Multiplicity formula). Let $\chi_\alpha$ be the character of the irreducible representation $\pi_\alpha$ and $\phi$ the character of the representation $\pi$ of a group $G$. Then

$$\frac{1}{|G|}\sum_{g \in G}(\chi_\alpha(g))^* \phi(g) = m_\alpha,$$

(18)

where $m_j$ is the multiplicity of the irreducible representation $\pi_j$ in the decomposition of $\pi$, so that $\pi$ is similar to a block diagonal matrix in the form

$$\pi(g) \simeq \bigoplus_{\alpha} \pi_\alpha(g) \otimes \mathbb{I}_{m_\alpha} \quad \forall g \in G,$$

(19)

with $\mathbb{I}_{m_\alpha}$ being the identity matrix on $\mathbb{C}^{m_\alpha}$.

For each irreducible subspace of $V$ we can choose a basis set $\{v_\alpha^j\}$, where $\alpha$ is a label of the irreducible representation (with dimension $\dim \alpha$) decomposing $\pi$ and $j \in \{1, \ldots, \dim \alpha\}$. Each vector $v$ in $V$ can then be written as its linear combination $v = \sum_\alpha \sum_{j=1}^{\dim \alpha} c_j^\alpha v_\alpha^j$. We can conversely identify the basis vector components of any vector $v$ by application of an appropriate projector $P_j^\alpha$, such that

$$P_j^\alpha v = c_j^\alpha v_\alpha^j,$$

where

$$P_j^\alpha = \frac{\dim \alpha}{|G|}\sum_{g \in G}(\chi_\alpha(g))^* \pi_j(g).$$

(20)

Note that, in order to construct these projectors, the knowledge of the sole diagonal elements of the corresponding irreducible representation $\pi_\alpha$ is sufficient. By having access to the character table only, it is still possible to project any vector onto distinct irreducible subspaces (up to multiplicity) by using

$$P^\alpha = \frac{\dim \alpha}{|G|}\sum_{g \in G}(\chi_\alpha(g))^* \pi(g).$$

(21)

**C. Schur’s Lemma**

Hereby we write one of the most important results in representation theory, namely, Schur’s Lemma. We will restrict it on finite-dimensional representations case.

**Lemma 12** (Schur’s Lemma). Let $\pi_\alpha$ and $\pi_\beta$ be two irreducible representations of a finite group $G$ of dimension $m$ and $n$ respectively, and $M$ an $m \times n$ matrix. If

$$\pi_\alpha(g) M \pi_\beta^{-1}(g) = M \quad \forall g \in G$$

(22)

then $\pi_\alpha$ and $\pi_\beta$ are equivalent irreducible representations or $M = 0$.

Furthermore, if

$$\pi_\alpha(g) M \pi_\alpha^{-1}(g) = M \quad \forall g \in G$$

(23)

then $M = \mu \mathbb{I}$, i.e., it is a scalar matrix.

**D. Construction of irreducible representations of semi-direct product groups**

It is possible to couple two groups to construct a new one using direct and semi-direct products. One can also obtain all their irreducible representations using knowledge about those of the original two groups alone. For direct products, the procedure is straightforward.

**Theorem 13** ([44], Theorem 10, Chapter 3). Each irreducible representation of a direct group $G_1 \times G_2$ is isomorphic to a representation $\pi_1 \otimes \pi_2$ with $\pi_1$ and $\pi_2$ being irreducible representations of group $G_1$ and $G_2$ respectively.

For a group generated by a semi-direct product $N \rtimes H$, a more sophisticated machinery is needed (cf. Refs. [44, 45]), and works only if the normal subgroup $N$ is also abelian, i.e., all elements commute with respect to the group operation. Assuming $N$ to be abelian, its irreducible representations $\{\chi_\alpha\}_\alpha$ are one-dimensional and carry an action of $G$ by

$$g \cdot \chi_\alpha(a) = \chi_\alpha(g^{-1}ag) \quad \forall a \in N \text{ and } g \in G.$$

(24)

Now, consider the orbits of the characters induced by the action of $H$ and choose a set of representatives $\{\chi_r\}$. For each $r$, let $H_r$ be the stabilizer subgroup of $\chi_r$ in $H$ and then define $G_r = N \cdot H_r$. Now extend $\chi_r$ to $G_r$ by

$$\chi_r(ah) = \chi(a) \quad \forall a \in N \text{ and } h \in H_r.$$ 

(25)

Let $\theta$ be an irreducible representation of $H_r$ and lift it to an irreducible representation $\tilde{\theta}$ of $G_r$ through the canonical projection $P: G_r \to G_r/N$. As a final step, compose the two representations and obtain a representation $\rho_{r,\tilde{\theta}}$ of the group $G$ by induction, i.e., $\rho_{r,\tilde{\theta}} = \text{Ind}_{G_r}^{G}(\chi_r \cdot \tilde{\theta})$. From Ref. [44] Proposition 25, we know that the so constructed representations $\rho_{r,\tilde{\theta}}$ are irreducible and exhaust all irreducible representations of $G$. Since we will only need the characters $\chi_{\rho_{r,\tilde{\theta}}}$ of the irreducible representations of $G$ to apply Schur’s Lemma, we will not elaborate what induced representations are. To obtain the sought characters, it suffices to make use of a Mackey-type formula,

$$\chi_{\rho_{r,\tilde{\theta}}}(s) = \frac{1}{|G_r|} \sum_{g \in G_r} \chi_r \cdot \tilde{\chi}_{\tilde{\theta}}(g^{-1}sg).$$

(26)

**E. Pauli-Liouville representation**

To represent density operators and quantum channel on $n$ qubits as vectors and matrices respectively, we will make use of the Pauli-Liouville representation with respect to Pauli basis. Let us pick

$$B := \left\{ \frac{1}{\sqrt{2^n}} \bigotimes_{\nu=1}^{n} \sigma_{\nu} : \sigma_{\nu} \in \{ \mathbb{I}, X, Y, Z \} \right\},$$

(27)

where $X, Y, Z$ are the Pauli matrices, as an orthonormal basis of $\text{GL}(\mathbb{C}^{2n})$ with respect to the Hilbert-Schmidt inner product.
\begin{align}
\langle A, B \rangle & := \text{Tr}[A^\dagger B]. \text{ Then we know that we can express any density operator } \rho \text{ and quantum channel } C \text{ respectively as }
\rho = \sum_{j=1}^{4^n} \rho_j \sigma_j \quad \text{and} \quad C(\rho) = \sum_{j=1}^{4^n} C(\sigma_j) \rho_j, \quad (28)
\end{align}
where \( \sigma_j \in B \) and \( \rho_j := \langle \sigma_j, \rho \rangle \), so that we can represent them as
\[
|\rho\rangle = \begin{pmatrix}
\rho_1 \\
\vdots \\
\rho_{4^n}
\end{pmatrix} \quad \text{and} \quad C_{jk} = \langle \sigma_j, C(\sigma_k) \rangle. \quad (29)
\]
In this way, we may transpose \( C(\rho) \) into a matrix-vector multiplication \( C|\rho\rangle \) and the concatenation of two channels \( D \) and \( C \) into a matrix multiplication \( DC \). Additionally, representing channels in matrix form will allow us to make use of Schur’s Lemma for matrix representations. We can analogously write a POVM \( E \) in the form
\[
\langle E \rangle = (E_1 E_2 \ldots E_{4^n}) \quad \text{with} \quad E_j = \langle E, \sigma_j \rangle. \quad (30)
\]
With this, the probability to obtain an outcome described by \( E \) when measuring \( \rho \) is \( p(E|\rho) = \text{Tr}[E\rho] = \langle E, \rho \rangle \).

\section*{F. Zassenhaus formula}

In order to justify our mathematical assumption through physical motivations, let us consider that the gate \( \tilde{U} \), which is the physical realization of the ideal gate \( U \), is obtained during the application of some Hamiltonian \( H \), perturbed for a fraction of time \( \Delta t \) (we denote the perturbed Hamiltonian as \( R \)), i.e., \( \tilde{U} = e^{-i(R\Delta t + HT)} \). Using the Zassenhaus formula \cite{Zassenhaus}, we can rewrite the implemented gate as
\[
\tilde{U} = e^{-iHT} e^{-iR\Delta t} \sum_{n=2}^{\infty} e^{C_n(HT,R\Delta t)} \quad (31)
\]
\[
= e^{-iHT} \left(I - iR\Delta t + \frac{\Delta t}{2} \right) + O(\Delta t^2), \quad (32)
\]
where
\[
\frac{\Delta t}{2} := \sum_{n=2}^{\infty} \sum_{n-1 \text{ times}} C_n[H,H,\ldots,H,R] \ldots]T^{n-1}, \quad (33)
\]
with the Zassenhaus coefficients \( c_n \) that can be recursively calculated for instance as in Ref. \cite{Zassenhaus}. This implies that the off-diagonal elements of the matrix \( \tilde{U} \) – computed in the \( n \)-basis of \( U \) – are of order \( \Delta t \), justifying our assumption on the noise \( \Lambda \).

\section*{G. First-order fitting model}

We will now take into account off-diagonal matrix entries. A feature of the protocol being of great relevance is that, by twirling the error channel over the symmetry group \( G \), we reduce the number of these off-diagonal matrix entries and so we drastically decrease the amount of parameters in the fitting model. Like in the main part of the letter, we write \( \Lambda^G = \Lambda_0 + \Lambda_{\text{off}} \), with \( \Lambda_0 \) being jointly diagonalizable with \( U \). Provided \( \Lambda_{\text{off}} = \{ \mu_{ij} \}_{i \neq j} \) to be “small” (i.e., the second-order perturbation being negligible), we can consider the first-order model
\[
F^{(1)}_{\text{avg}}(\ell, \rho) = F^{(0)}_{\text{avg}}(\ell, \rho) + \sum_{i \neq j} \sum_{p=0}^{\ell-1} (\lambda_i d_i)^p (\lambda_j d_j)^{\ell-p-1} \zeta_{ij}, \quad (34)
\]
with \( \zeta_{ij} := \mu_{ij} d_j \text{ Tr}[E\Lambda(v_i)|\rho, v_j] \) and the indices \( i, j \) labeling the elements within the support of \( \rho \). This expression may be re-formulated into a simpler form, e.g., using the geometric series formula we obtain
\[
F^{(1)}_{\text{avg}}(\ell, \rho) = F^{(0)}_{\text{avg}}(\ell, \rho) + \sum_{i \neq j} (\lambda_i d_i)^{\ell} - (\lambda_j d_j)^{\ell} \lambda_j d_j - \lambda_i d_i \zeta_{ij}. \quad (35)
\]
As already mentioned, since we twirled over the symmetry group and so \( \Lambda^G \) is block-diagonal, a number of \( \mu_{ij} \) (and hence the corresponding \( \zeta_{ij} \)) can be set to 0 in advance. More precisely, when a representation of the symmetry group is written as a direct sum of irreducible representations as
\[
\pi(g) = \bigoplus_{\alpha \text{irrep}} \mathbb{I}_{m_\alpha} \otimes \pi_\alpha(g), \quad (36)
\]
where \( m_\alpha \) is the multiplicity of the irreducible representation \( \pi_\alpha \), two matrices \( X \) and \( Y \) which are both commuting with \( \pi(g) \) assume the form
\[
X = \bigoplus_{\alpha} x^\alpha \otimes \mathbb{I}_{\text{dim } \alpha} \quad \text{and} \quad Y = \bigoplus_{\alpha} y^\alpha \otimes \mathbb{I}_{\text{dim } \alpha}, \quad (37)
\]
where \( x^\alpha, y^\alpha \) are square matrices with \( \text{dim } x^\alpha = \text{dim } y^\alpha = m_\alpha \). If \( X \) is normal, one can then choose a basis such that all \( x^\alpha \) are diagonal (so that \( X \) will assume a diagonal form), while \( Y \) will maintain a similar form \( Y = \bigoplus_{\alpha} y^\alpha \otimes \mathbb{I}_{\text{dim } \alpha} \). Hence, in our case, while diagonalizing \( U \) (from the Pauli-Liouville representation), \( \Lambda^G \) maintains a form as in Eq. \cite{Zassenhaus}.

\section*{H. Connecting to the average gate fidelity}

For a quantum channel \( \mathcal{E} \) and a unitary operation \( \mathcal{U} \), the gate fidelity between these two quantities for a pure state \( \phi \) is given by
\[
F_{\mathcal{E},\mathcal{U}}(\phi) := \text{Tr}[\mathcal{U}(|\phi\rangle \langle \phi|) \mathcal{E}(|\phi\rangle \langle \phi|)] \quad (38)
\]
and defining \( \Lambda = \mathcal{U}^\dagger \circ \mathcal{E} \) one has
\[
F_{\mathcal{E},\mathcal{U}}(\phi) = F_{\Lambda,\mathcal{E}}(\phi) = \text{Tr}[|\phi\rangle \langle \phi| \Lambda(|\phi\rangle \langle \phi|)], \quad (39)
\]
thereby quantifying the noise channel \( \Lambda \) for the implementation \( \mathcal{E} \) of \( \mathcal{U} \).
The *average gate fidelity* is then obtained by integrating this quantity over the Haar measure on pure states, that is,

\[
\mathbb{E}(F_{E,U}) = \mathbb{E}(F_{\Lambda,I}) := \int_{\text{Haar}} \text{Tr} [\psi \langle \phi | \Lambda (|\phi\rangle \langle \phi|)] \, d\phi.
\]

Conversely, the *entanglement fidelity* of a quantum channel \( \mathcal{E} \), defined as

\[
F_{\text{ent}}(\mathcal{E}) := \langle \psi | (I \otimes \mathcal{E})(|\psi\rangle \langle \psi|) |\psi\rangle,
\]

with \(|\psi\rangle\) being a maximally entangled state vector, can be written as \(47\)

\[
F_{\text{ent}}(\mathcal{E}) = d^{-3} \sum_j \text{Tr}[V_j^\dagger \mathcal{E}(V_j)],
\]

for any orthonormal basis \( \{V_j\} \) such that \( \text{Tr}[V_j V_k] = \delta_{j,k} \) (in the case of \( n \) qubits, \( d = 2^n \)). The average gate fidelity of \( \mathcal{E} \) is then linked to this quantity by \(47\)

\[
\mathbb{E}(F_{E,I}) = \frac{d F_{\text{ent}}(\mathcal{E}) + 1}{d + 1} = \frac{\sum_j \text{Tr}[V_j^\dagger \mathcal{E}(V_j)] + d^2}{d(d + 1)},
\]

so that the average gate fidelity of the twirled error channel \( \Lambda^G \) is related to the parameters \( \{ \lambda_j \} \), obtained in the fitting model in Eq. (7) from the main part of the letter by

\[
\mathbb{E}(F_{\Lambda,G,I}) = \frac{\sum \lambda_j + d}{d(d + 1)}.
\]

Now the question is what information about the original noise channel we can extract from the twirled channel \( \Lambda^G \). In fact they are the same, since the entanglement fidelity is invariant under twirling over the symmetry group \( G \). Let us rewrite

\[
F_{\text{ent}}(\Lambda^G) = d^{-3} \sum_j \text{Tr}[V_j^\dagger \Lambda^G(V_j)]
\]

\[
= \frac{d^{-3}}{|G|} \sum_{k=1}^{|G|} \sum_j \text{Tr}[V_j^\dagger g_k (\Lambda (g_k V_j g_k^\dagger) g_k)]
\]

\[
= \frac{d^{-3}}{|G|} \sum_{k=1}^{|G|} \sum_j \text{Tr}[(W_j^k)^\dagger \Lambda (W_j^k)],
\]

where we denote \( W_j^k = g_k V_j g_k^\dagger \) and used cyclicity of the trace. Since \( W_j^k \) is again an orthogonal basis with respect to the Hilbert-Schmidt inner product (i.e., \( \text{Tr}[(W_j^k)^\dagger W_j^l] = d \delta_{j,l} \forall k \)), then \( d^{-3} \sum_j \text{Tr}[(W_j^k)^\dagger \Lambda (W_j^k)] = F_{\text{ent}}(\Lambda) \) so that

\[
F_{\text{ent}}(\Lambda^G) = \frac{1}{|G|} \sum_{k=1}^{|G|} F_{\text{ent}}(\Lambda) = F_{\text{ent}}(\Lambda)
\]

and hence

\[
\mathbb{E}(F_{\Lambda,I}) = \mathbb{E}(F_{\Lambda^G,I}).
\]
\[
\sigma_t^2 = \Delta t^2 (E^{\otimes 2}) \sum_{j=1}^{\ell} \frac{1}{|G|} \sum_{B \in G} (U \otimes U)^{t-j} (B^\dagger QB \otimes B^\dagger QB)(U \otimes U)^j - \sum_{j=1}^{\ell} (U \otimes U)^{t-j} (Q^G \otimes Q^{\dagger})(U \otimes U)^j |\rho^{\otimes 2}\rangle + O(\ell^2 r^2 d^4).
\]

The first term can be bounded as in Ref. [50] using diamond norm properties and Ref. [50] Proposition 9 with \(4d(d+1)\ell r\). Again following that argument, the terms of order \(O(\Delta t^3 Q^4)\) and \(O(\Delta t^4 Q^4)\) are \(O(\ell^2 r^2 d^4)\). Knowing the structure of \(Q^G\) from the analysis of the symmetry group \(G\), we can upper bound the number of non-zero terms as

\[
\sum_{\alpha} m_\alpha d_\alpha \leq \max_{\alpha} m_\alpha \sum_{\alpha} m_\alpha d_\alpha = \max_{\alpha} m_\alpha d^2.
\]

From now on, we denote \(m = \max_{\alpha} m_\alpha\) and \(q = \max_{i,j} q_{i,j}\), the largest matrix entry of \(Q\) that we assume being independent of \(d\). The second term in expression [54] obeys to the inequality

\[
(E^{\otimes 2}) \sum_{j=1}^{\ell} (U \otimes U)^{t-j} (Q^G \otimes Q^{\dagger})(U \otimes U)^j |\rho^{\otimes 2}\rangle \leq \ell q^2 m^2 d^4.
\]

Using

\[
\text{Tr}[\Lambda] = d(d+1)\Xi(F) - d
\]

follows

\[
\Delta t = -r \frac{d(d+1)}{\text{Tr}[Q]},
\]

and so \(\Delta t = O(r)\) since we assumed \(\text{Tr}Q = \Theta(d^2)\). Hence, second term of Eq. (54) is \(O(m^2 \ell r^2 d^4)\). Summarizing gives a bound for the variance as

\[
\sigma_t^2 \leq 4d(d+1)\ell r + O(\ell^2 r^2 d^4) + O(m^2 \ell r^2 d^4),
\]

where the second term dominates the third one for \(\ell \gg m^2\), i.e., in this regime the bound is exactly equivalent to the one of Ref. [50] Theorem 10]. This bound however is probably not tight, and we are interested whether a bound similar to the one provided in Ref. [51] can be obtained.

**K. Example of tensor copies of \(T\)-gates**

Starting from this part of the appendix we will illustrate the application of our scheme to tensor copies of the \(T\)-gate, one of the most relevant quantum gates, which together with the \(H\), \(S\) and CNOT gates gives rise to a universal quantum circuit. Specifically within the context of fault tolerant quantum computing, this situation is of paramount importance. First, we are going to depict the irreducible decomposition up to four tensor copies of this gate in order to get a feeling on the scalability and necessary resources for this method. We give in the following the step-by-step sequence according to the procedure described in Appendix D.

[1] Produce the \(n\)-Kronecker product group, denoted by \(A_n\), of the local abelian symmetry group

\[
\left\{ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \right\},
\]

which is isomorphic to the cyclic group of order 4, \(\mathbb{Z}_4\).

[2] Construct representation of the symmetric group \(S_n\) permuting the local subsystems.

[3] Construct the full symmetry group \(G\) as a semi-direct product of \(A_n\) and \(S_n\) by multiplying the respective \(4^n\)-dimensional matrix representations. Each \(g \in G\) is given by \(g = a.\sigma\), with \(a \in A_n, \sigma \in S_n\).

[4] From the character table of \(Z_4\),

\[
\begin{array}{cccc}
Z_4 & \gamma & \gamma^2 & \gamma^3 \\
\chi_0 & 1 & 1 & 1 \\
\chi_1 & 1 & -1 & -1 \\
\chi_2 & 1 & -1 & 1 \\
\chi_3 & 1 & 1 & -1 \\
\end{array}
\]

construct the character table of \(A_n\) by taking the product of the respective characters

\[
\chi_{c_1,c_2,\ldots,c_n}(\ell_1,\ell_2,\ldots,\ell_n) := \chi_{c_1}(\ell_1)\chi_{c_2}(\ell_2)\cdots\chi_{c_n}(\ell_n),
\]

where \(\ell_j \in \mathbb{Z}_4\) and \(c_j\) is the label representing the irreducible representation.

[5] Divide the characters of \(A_n\) into orbits with respect to the action of \(S_n\) given by

\[
\sigma.\chi(a)_{c_1,c_2,\ldots,c_n} := \chi(\sigma^{-1}a\sigma)_{c_1,c_2,\ldots,c_n}.
\]

In this particular case, the action of \(S_n\) works as a permutation of the labels of the irreducible representations, i.e.,

\[
\sigma.\chi(a)_{c_1,c_2,\ldots,c_n} = \chi(a)_{\sigma(c_1,c_2,\ldots,c_n)}.
\]

Choose for each orbit a representative element, for instance \(\chi(a)_{c_1,c_2,\ldots,c_n}\) with \(c_1 \leq c_2 \leq \cdots \leq c_n\), building a set \(\{\chi_j\}_j\).
For each representative element $\chi_j$, find the stabilizer group $H_j$ as a subgroup of $S_n$. For each irreducible representation $\pi$ of $H_j$, write an irreducible representation of the subgroup $G_j := A_n \cdot H_j$ of $G$ by

$$\tilde{\rho}_\pi^j(a, g_j) = \chi_j(a) \cdot \pi(g_j).$$

Obtain the characters of the representation $\tilde{\rho}_\pi^j$ of $G$ induced by $\tilde{\rho}_\pi^j$ with the Mackey-type formula,

$$\chi_{\tilde{\rho}_\pi^j}(s) = \frac{1}{|G_j|} \sum_{t \in G} \chi_{\tilde{\rho}_\pi^j}(t^{-1}st),$$

and obtain the irreducible representation multiplicity $m_j^n$ in the decomposition of the Pauli-Liouville representation of $G$ with the formula

$$m_j^n = \frac{1}{|G|} \sum_{g \in G} \left( \chi_{\tilde{\rho}_\pi^j}(g) \right)^* \phi(g),$$

where $g \mapsto \phi(g)$ is the trace of $g$ in Pauli-Liouville representation.

In case of $n = 4$, for instance, there are 256 different irreducible representations of $A_4$ and five stabilizer groups: the full permutation group $S_4$ for the irreducible representations of the form $\chi_{a,a,a,a}$, $a \in 0, 1, 2, 3$, giving rise to $4 \cdot 5 = 20$ irreducible representations for $G$, $S_3$ for the irrep of $a < b$, $\chi_{a,a,b,b}$ with $a < b$, giving rise to $12 \cdot 3 = 36$ new irreducible representations, $S_2 \times S_2$ (isomorphic to the Klein four-group) for $\chi_{a,a,b,b}$ with $a < b$, so that a total of $6 \cdot 4 = 24$ irreducible representations of $G$ are derived, again representative elements $\chi_{a,a,b,b}$, $\chi_{a,a,b,c}$, $\chi_{a,b,b,c}$, $\chi_{a,b,c,c}$ with $a < b < c$ have stabilizer $S_2$, producing additional $12 \cdot 2 = 24$ irreducible representations; finally, the single element $\chi_{0,1,2,3}$ represents the sole orbit with trivial stabilizer. Hence, we have in total 105 different induced irreducible representations of $G$ whose characters are obtained using Eq. (64). As one can observe in Table IV, only 22 of these irreducible representations decompose the twirled noise matrix, and the trivial representation has the highest multiplicity.

Results for $n \leq 4$

We report in Tables I-IV the irreducible decompositions for up to four tensor copies of the $T$-gate. The superscripts of $\chi$ label the irreducible representations of $A_n$, while after the semicolon we denote the irreducible representation of the stabilizer group, where $e$ denotes the trivial representation, $std$ the standard representation for all subgroups of $S_4$, $ker_a$ the kernel $a$ representation of the Klein four-group isomorphic to $S_2 \times S_2$, while $2dim$ denotes the 2-dimensional representation of $S_4$. We note that $\chi_2$ never appears in the decomposition, and that the highest multiplicity, being $n + 1$, is always related to the trivial representation of the full group $G$. Additionally, we note that exploiting Schur’s Lemma and the above consideration, the number of distinct $\lambda_j$ to be fitted when benchmarking copies of the $T$-gate is $\sum_{\alpha \in \text{irrep}} m_\alpha$, i.e., from 1 to 4 qubits, this number is 4, 11, 24, 46.

L. Classical recovery and estimation methods

In this section, we give details on the our numerical methods employed to recover the average fidelity from the measurement data provided by our protocol. In principle, we could try to obtain the parameters directly by a non-linear fitting approach along the lines of the variable projection algorithm that separates fitting of linear and non-linear parameters [52]. However, given the fact that the quantities we want to obtain correspond to the estimation of different decay rates in the data set, we are going to use instead a matrix pencil method for the extraction of signal poles developed in the context of signal processing [53, 54]. Due to the random nature of the sampling paths, this is supplemented by a bootstrapping approach in order to get reliable estimates on these parameters. We will continue describing these two components of our methodology in detail now, before commenting on the single and two $T$-gate examples described in the main text.

1. Matrix pencil methods

Key to the functioning of our scheme is the use of sophisticated methods of estimation which we lay out here. According to [44], we can express the average fidelity $E(F_0(x_i))$ of the twirled channel in terms of the model parameters $\lambda_j$ as

$$E(F_0(x_i)) = \frac{\sum \lambda_j + d}{d(d + 1)}.$$  

The relation between the model parameters $\lambda_j$ and the measurement data on the other hand is given by the zeroth-order fitting model

$$F_{\text{avg}}(0, \rho) = \sum_{j=1}^{4^n} (\lambda_j d_j)^i \xi_j.$$ 

From an abstract point of view this means that up to higher order terms, for each $\ell = 1, \ldots, \ell_{\text{max}}$, the measurement result $F_\ell$ can be expressed as a sum exponentially decaying terms of the form

$$F_\ell = \sum_{j=1}^M \xi_j d_j^\ell$$

where we set $x_j = \lambda_j d_j$. Recovering the parameters $x_j$ from such a noisy data set is a well studied problem in the context of signal reconstruction going back to the work by Prony. Modern algorithms known as the Estimation of signal parameters...
via rotational Invariance Techniques (ESPRIT) rely on feature extraction via singular value decompositions and matrix pencils [55]. For a recent review and details of the construction see, e.g., Ref. [56]. In the following, we give a short overview over the algorithm.

In order to extract at most $M_{\text{max}}$ signal poles $x_j$ from \( \{ F(\ell) \}_{\ell=0}^{\ell_{\text{max}}-1} \), we first form the \( 2L_{\text{max}} - M_{\text{max}} \times M_{\text{max}} + 1 \) Hankel matrix $H_{\ell,k} = F(\ell + k)$ and compute its singular value decomposition

\[
H = UDV^*.
\]  

If there were no noise in the data, the number of non-zero singular values of $H$ would correspond directly to the number of unique \( \{ x_j \} \) in [68]. However, in the presence of noise, $H$ will typically feature full rank and we have to fix a threshold $\sigma_{\text{min}}$ for the singular values to obtain a rank $M$ approximation of $H$ in order to extract $M \leq M_{\text{max}}$ poles for the approximation of our measurement data. Let us denote by $W$ the $M \times M_{\text{max}} + 1$ matrix formed by the first $M$ rows of $V^*$ and set the $M_{\text{max}} \times M$ matrices $V_0$ and $V_1$ equal to

\[
(V_0)_{\ell,k} = M_{k,\ell+i}, \quad \ell = 1, \ldots, M_{\text{max}}, \quad k = 1, \ldots, M.
\]

The estimate for the signal poles $x_j$ can now be computed as the $M$ eigenvalues of the matrix $(V_0)^{-1} \cdot V_1$, where the inverse of $V_0$ is defined as its Moore-Penrose pseudo-inverse. In this way, we can extract from (67) the parameters \( \{ x_j \} = \{ \lambda_j d_j \} \).

Now in principle, we would be left with the problem of matching the right $x_j$ with the correct $d_j$ in order to obtain the parameters $\lambda_j$. However, since typical quantum gates and in particular the $T$-gate have eigenvalues which are close to being roots of unity, we can exploit this property to circumvent this problem. Namely, assuming that we can find an $\tau$ such that $d_j^\tau = 1$ for all $j$, we can partition our measurement data \( \{ F(\ell) \}_{\ell=0}^{\ell_{\text{max}}-1} \) into $\tau$ subsets of the form \( \{ F(r), F(r+\tau), F(r+2\tau), \ldots \} \) with $r = 1, \ldots, \tau$. In each of these subsets [67] reads as

\[
F_\tau(\ell) = \sum_j \xi_j d_j^\ell \cdot (d_j^\tau)^{\ell} = \sum_j \tilde{\xi}_j, (\lambda_j^\tau)^\ell,
\]  

which is again of the form (68) with $x_j = \lambda_j^\tau$ and $\tilde{\xi}_j = \xi_j d_j^\tau$. Now using the reconstruction method described before, we can extract from this data $\lambda_j^\tau$ and in turn obtain $d_j$ by taking the $\tau$-s-root. In terms of data collection from an experiment, we now have two options: we can restrict the set of data points, i.e., measured expectation values, to $\ell = 1, \tau, 2\tau, \ldots$ or we can also collect data at intermediate points and extract the poles from the combined Hankel matrix $[H_1, H_2, \ldots, H_\tau]$ in the way described before according to a multi-channel signal reconstruction approach [57].

2. Restriction to symmetry subspaces

In this subsection, we will explain how the restriction to symmetry subspaces will lead to a robust numerical recovery procedure. Under our standing assumption that the twirled noise channel $\Lambda U$ is almost jointly diagonalizable with the target unitary channel $U$, it follows directly that $\Lambda U$ will also approximately preserve the invariant subspaces of the symmetry group $G$. For our protocol this means that by choosing an appropriate initial states $\rho$ supported on such an invariant subspace, $(\Lambda U)^\ell(\rho)$ will still be approximately located there.

This observation serves us in two ways: On the one hand, we can get additional information about the performance of the benchmarked operation with respect to a specific subspace, i.e., we can identify the subspaces on which the errors occur. On the other hand, we reduce the number of signal parameters $\lambda_j$ we have to extract from our data considerably if we restrict the initial state to a particular subspace. This becomes particularly important when we come close to an optimal implementation where the $\lambda_j$ become closer and closer to being degenerate. To apply this approach, previously developed to tackle multi-parameters fitting models for finite groups [57], we first construct the seven projectors linked to the irreducible representations in Table II and then take the corresponding eigenvectors as a basis of the invariant subspaces. Subsequently, we need to construct from these vectors a set of density operators such that we can address each irreducible subspace at

<table>
<thead>
<tr>
<th>Irreducible representation</th>
<th>Dim</th>
<th>Multip.</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\chi_0$</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$\chi_1$</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>$\chi_3$</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Table II. Two $T$-gates decomposition.

<table>
<thead>
<tr>
<th>Irreducible representation</th>
<th>Dim</th>
<th>Multip.</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\chi_0$, $\chi_0$, $e$</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>$\chi_1$, $\chi_1$, $e$</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>$\chi_3$, $\chi_3$, $e$</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

Table I. This and the subsequent three tables depict the irreducible decompositions of the symmetry group $G$ of multiple tensor copies of the $T$-gate channel. The superscripts of $\chi$ label the irreducible representations of $A_4$, the word after the semicolon the irreducible representation of the stabilizer group: $e$ denotes the trivial representation, $\text{sgn}$ the sign representation, $\text{std}$ the standard representation, $\ker$ the Kernel a representation of the Klein four-group, $2\dim$ the 2-dimensional representation of $S_4$.
least once and target only few of those subspaces in a single iteration. This choice is clearly not unique; for our numerics, we selected as input state the density matrices given in Section M. It is a key insight to the functioning of the method that we can address single or a few irreducible subspaces in each iteration to arrive at a reliable and robust method that is able to reliably discriminate between close poles.

3. Bootstrapping for parameter estimation

Here, we give further details on the our numerical methods used to extract the average fidelity from the measurement data provided by our protocol. The starting point is the observation that the data obtained experimentally by executing our scheme contain more information than necessary for the model: Instead of having access to the observed average survival probabilities for a given execution length \( \ell \) solely, our protocol actually provides this information at the level of each of the randomly chosen sample paths of length \( \ell \) individually. This insights motivates the use of standard methods in statistical estimation called bootstrapping procedures \(^{59}\) in order to reliably extract the average fidelity. Bootstrapping techniques refer to random sampling methods with replacement, designed in order to assign measures of accuracy to sample estimates.

For this, note that the sampling paths both with respect to the sequence length \( \ell \) as well as with respect to the given realization of length \( \ell \) are chosen independently. Hence, given the set of measured survival probabilities \( \{ F_{k_{\ell,q}} \} \), where \( 1 \leq \ell \leq \ell_{\text{max}} \) denotes the circuit length and \( k_{\ell,q} \) the \( q \)-th randomly chosen sample sequence of symmetry gates for length \( \ell \), we are going to resample this set of data with respect to \( \ell \). More precisely, in order to create a single bootstrap sample, we pick for each fixed \( \ell \) a random subset with replacement of \( m \) elements from \( \{ F_{k_{\ell,q}} \} \) and compute their average with respect to \( q \). For each of these resampled sequences, we compute the approximated average fidelity, according to our fitting model and matrix pencil methods described in Appendix [L 1]. The final estimate for the averaged fidelity is then obtained as average over all taken bootstrap samples.

### M. Numerical recovery

In this section, we apply the recovery procedure detailed in Appendix [L 1] for two significant examples of practical relevance that are problematic to handle with the common approach to randomized benchmarking: A single \( T \)-gate and the tensor product of two \( T \)-gates.

#### 1. Single \( T \)-gate-case

We describe here the numerics reported in the main text in greater detail. First, we consider the case of a single \( T \)-gate that is generated by the noisy Hamiltonian

\[
H_T = \frac{\pi}{8} \sigma_z - \varepsilon \sigma_x
\]  

(71)

with noise parameter \( \varepsilon > 0 \). The four eigenvalues of the \( T \)-gate channel including multiplicities are given by \( \{ 1, 1, (1 + i)/\sqrt{2}, (1 - i)/\sqrt{2} \} \). Accordingly, we have to extract four decay parameters \( \lambda_j \) to estimate the average fidelity from \( \{ \ell \} \). As described in Appendix [L 1] we make use of the fact that the \( T^8 = 1 \) and hence we can extract the parameters \( \lambda_j \) by described matrix pencil approach. By exploiting the symmetry of the \( T \)-gate, we can obtain information in three invariant subspaces by running our protocol with the initial

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>( \chi_0, \chi_0; \psi )</td>
<td>1</td>
<td>4</td>
<td>( \chi_0, \chi_0; \chi_3; \psi )</td>
<td>3</td>
<td>3</td>
<td>( \chi_0, \chi_0, \chi_3; \psi )</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>( \chi_1, \chi_1; \psi )</td>
<td>1</td>
<td>1</td>
<td>( \chi_0, \chi_1; \psi )</td>
<td>3</td>
<td>2</td>
<td>( \chi_0, \chi_0, \chi_3; \psi )</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>( \chi_3, \chi_3; \psi )</td>
<td>1</td>
<td>1</td>
<td>( \chi_1, \chi_1; \psi )</td>
<td>3</td>
<td>1</td>
<td>( \chi_0, \chi_1, \chi_3; \psi )</td>
<td>6</td>
<td>2</td>
</tr>
<tr>
<td>( \chi_0, \chi_0, \chi_0; \psi )</td>
<td>2</td>
<td>2</td>
<td>( \chi_0, \chi_3, \psi )</td>
<td>3</td>
<td>2</td>
<td>( \chi_0, \chi_1, \chi_3; \psi )</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>( \chi_0, \chi_1, \chi_1; \psi )</td>
<td>3</td>
<td>3</td>
<td>( \chi_1, \chi_3, \psi )</td>
<td>3</td>
<td>1</td>
<td>( \chi_0, \chi_1, \chi_3; \psi )</td>
<td>6</td>
<td>2</td>
</tr>
</tbody>
</table>

Table III. Three \( T \)-gates decomposition.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>( \chi_0, \chi_0; \psi )</td>
<td>1</td>
<td>5</td>
<td>( \chi_1, \chi_1, \chi_3; \psi )</td>
<td>3</td>
<td>3</td>
<td>( \chi_0, \chi_0, \chi_3; \psi )</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>( \chi_1, \chi_1; \psi )</td>
<td>1</td>
<td>1</td>
<td>( \chi_0, \chi_0, \chi_3; \psi )</td>
<td>3</td>
<td>2</td>
<td>( \chi_0, \chi_1, \chi_3; \psi )</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>( \chi_3, \chi_3; \psi )</td>
<td>1</td>
<td>1</td>
<td>( \chi_0, \chi_3, \psi )</td>
<td>3</td>
<td>2</td>
<td>( \chi_0, \chi_1, \chi_3; \psi )</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>( \chi_0, \chi_0, \chi_0; \psi )</td>
<td>2</td>
<td>2</td>
<td>( \chi_0, \chi_0, \chi_3; \psi )</td>
<td>3</td>
<td>2</td>
<td>( \chi_0, \chi_1, \chi_3; \psi )</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>( \chi_0, \chi_0, \chi_0; \psi )</td>
<td>3</td>
<td>3</td>
<td>( \chi_0, \chi_0, \chi_0; \psi )</td>
<td>3</td>
<td>2</td>
<td>( \chi_0, \chi_1, \chi_3; \psi )</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>( \chi_0, \chi_0, \chi_0; \psi )</td>
<td>4</td>
<td>4</td>
<td>( \chi_0, \chi_0, \chi_0; \psi )</td>
<td>3</td>
<td>2</td>
<td>( \chi_0, \chi_1, \chi_3; \psi )</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>( \chi_0, \chi_1, \chi_1; \psi )</td>
<td>4</td>
<td>2</td>
<td>( \chi_0, \chi_0, \chi_0; \psi )</td>
<td>3</td>
<td>2</td>
<td>( \chi_0, \chi_1, \chi_3; \psi )</td>
<td>3</td>
<td>1</td>
</tr>
</tbody>
</table>

Table IV. Four \( T \)-gates decomposition.
we consider the perturbed Hamiltonian

\[ \sigma \]

with the additional noise-term \( \lambda \) responding decay parameters \( \epsilon \) extracted from bootstrapping over \( N = 100 \) sequences of length the given length \( \ell \). In each of these subspaces, we extract the corresponding decay parameters \( \epsilon \) (they are reported below this paragraph). In each of these subspaces, we extract the corresponding decay parameters \( \epsilon \) as well as depending on the maximal protocol length. Similar to the single \( T \)-gate case, we see that \( \epsilon \leq 0.01 \) already \( \ell_{\text{max}} = 800 \) gives satisfactory results. However, in order to obtain meaningful lower bounds for larger values of \( \epsilon \), we have to double \( \ell_{\text{max}} \) to 1600.

2. Two \( T \)-gate case

In the case of two \( T \)-gates applied in parallel to two qubits, we consider the perturbed Hamiltonian

\[ H_\epsilon = \frac{\pi}{8} (\sigma_z \otimes I + I \otimes \sigma_z - \epsilon \sigma_x \otimes \sigma_z) \]  

(73)

with the additional noise-term \( \sigma_x \otimes \sigma_z \). In order to extract the decay parameters \( \lambda_j \), we follow the approach of the single \( T \)-gate, the main difference being that we now choose the initial state among eight density matrices supported on different symmetry subspaces (they are reported below this paragraph). In each of these subspaces, we extract the corresponding decay parameters \( \lambda_j \), which after bootstrapping leads us to an estimate of the desired average fidelity. Fig. 1 (b) depicts these estimates both in relation to the perturbation strength \( \epsilon \) as well as depending on the maximally protocol length. Similar to the single \( T \)-gate case, we see that \( \epsilon \leq 0.01 \) already \( \ell_{\text{max}} = 800 \) gives satisfactory results. However, in order to obtain meaningful lower bounds for larger values of \( \epsilon \), we have to double \( \ell_{\text{max}} \) to 1600.

We now provide the quantum states used as input for our numerics. Each of them combines the totally mixed state with some of the basis vectors obtained by the projectors onto the irreducible subspaces. To obtain the diagonal elements of \( \Lambda \) connected to the trivial subspaces, we choose the states

\[ \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & \frac{1}{4} & 0 \\ 0 & 0 & 0 & \frac{1}{4} \end{pmatrix}, \quad \begin{pmatrix} \frac{1}{4} & 0 & 0 & -\frac{1}{4} \\ 0 & \frac{1}{4} & 0 & 0 \\ 0 & 0 & \frac{1}{4} & 0 \\ -\frac{1}{4} & 0 & 0 & \frac{1}{4} \end{pmatrix} \]

and measuring the corresponding survival probability. Fig. 1 (a) shows the extracted estimates of the average fidelity depending on the strength of the perturbation \( \epsilon \) and the maximal sequence length of the protocol. It can be seen that we achieve a good agreement with the analytical value of the average fidelity even for short protocol sequences in the case of perturbations smaller than \( \epsilon \leq 0.01 \). However, by increasing the sequence length to \( \ell_{\text{max}} = 1000 \), we even achieve satisfactory estimates starting from \( \epsilon \leq 0.1 \).

\[ \rho \in \left\{ \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \frac{1}{2} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \right\} \]  

(72)

is a combination of the totally mixed state and the one belonging to the irrep \( \chi_0, \chi_0; e \). With the first of the following two density matrices,

\[ \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & \frac{1}{4} & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{4} \end{pmatrix}, \quad \begin{pmatrix} \frac{1}{4} & 0 & -\frac{1}{4} & 0 \\ \frac{1}{4} & 0 & -\frac{1}{4} & 0 \\ \frac{1}{4} & 0 & -\frac{1}{4} & 0 \\ \frac{1}{4} & 0 & -\frac{1}{4} & 0 \end{pmatrix} \]

we obtain two poles for \( \chi_0, \chi_1; e \) and two for \( \chi_0, \chi_3; e \) (and again the trivial one). With the second operator with get the other two poles of these two irreducible representations. The last density matrix,

\[ \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & \frac{1}{4} & \frac{1}{4} & 0 \\ 0 & \frac{1}{4} & \frac{1}{4} & 0 \\ 0 & 0 & 0 & \frac{1}{4} \end{pmatrix}, \quad \begin{pmatrix} \frac{1}{4} & 0 & 0 & 0 \\ 0 & \frac{1}{4} & \frac{1}{4} & 0 \\ 0 & \frac{1}{4} & \frac{1}{4} & 0 \\ 0 & 0 & 0 & \frac{1}{4} \end{pmatrix} \]

contains the basis vectors of the 2-dim irrep \( \chi_1, \chi_3; e \). With this selection, we cover every irreducible subspace and so we can extract all the \( \lambda_j \) elements, addressing at most five of them at one time.


[18] The supplements cite Refs. [44–57, 59].


