Statistical correlations between locally randomized measurements: a toolbox for probing entanglement in many-body quantum states

A. Elben,[*] B. Vermersch, C. F. Roos, and P. Zoller
Center for Quantum Physics, University of Innsbruck, Innsbruck A-6020, Austria and
Institute for Quantum Optics and Quantum Information,
Austrian Academy of Sciences, Innsbruck A-6020, Austria

We develop a general theoretical framework for measurement protocols employing statistical correlations of randomized measurements. We focus on *locally* randomized measurements implemented with *local* random unitaries in quantum lattice models. In particular, we discuss the theoretical details underlying the recent measurement of the second Rényi entropy of highly mixed quantum states consisting of up to 10 qubits in a trapped-ion quantum simulator [Brydges et al., arXiv:1806.05747]. We generalize the protocol to access the overlap of quantum states, prepared sequentially in an experiment. Furthermore, we discuss proposals for quantum state tomography based on randomized measurements within our framework and the respective scaling of statistical errors with system size.

I. INTRODUCTION

The development of intermediate- and large scale quantum simulators [1], consisting of tens of individually controlled quantum particles, requires new tools to probe and verify complex many-body quantum systems [2–5]. A key feature of composite quantum systems, in particular quantum lattice models, is bipartite entanglement which can be accessed by the measurement of Rényi entropies [6]. In spin models with a few degrees of freedom, Rényi entropies can be determined from tomographic reconstruction of the quantum state of interest [7–10]. In systems realizing one-dimensional Bose Hubbard models, the measurement of the second Rényi entropy has been demonstrated in remarkable experiments [11, 12]. Here, two identical copies of the quantum state have been prepared and the second Rényi entropy has been determined from an interference experiment [13–15].

In Ref. [16] we have demonstrated in a theory-experiment collaboration a new protocol in which the second order Rényi entropy is inferred from statistical correlations of locally randomized measurements [17]. Here, a spin model in a trapped-ion quantum simulator was realized and the generation of entanglement during quench dynamics was monitored. The measurement protocol to access the second Rényi entropy was based on only *local operations on individual spins and a single instance of the quantum state*. It required, albeit an exponential scaling with the number of degrees of freedom, a significantly lower number of measurements than standard quantum state tomography [16]. This measurement protocol is thus immediately applicable in a broad class of quantum simulators, realizing spin models, with single site readout and control. In particular, we have in mind systems based on trapped-ions [16, 18], Rydberg atoms [19–22] and superconducting qubits [23–26] in arbitrary spatial dimensions. Moreover, our protocol can straightforwardly be applied to extended systems such as quantum networks.

The key ingredient for the protocols described in this paper are statistical correlations between randomized measurements. We develop a general mathematical formalism to evaluate such correlations and, equipped with this toolbox, elaborate on the theoretical details behind the protocol realized in Ref. [16].

In general, a random measurement on a (reduced) quantum state ρ is performed by the application of random unitary U, sampled from an appropriate ensemble (see below), and the subsequent measurement of the expectation value $\langle O\rangle_U = \mathrm{Tr}\left[U\rho U^\dagger O\right]$ of a fixed observable O. In this paper, we focus on spin models and *locally* randomized measurements where the random unitaries are of the form $U = \otimes_i U_i$ with the U_i independent random spin rotations sampled from unitary designs (in particular the circular unitary ensemble (CUE)) [16, 17]. Furthermore, we provide an in-depth comparison to protocols based on *globally* randomized measurements [17, 27] where global random unitaries U are sampled from the unitary designs defined on the entire Hilbert space. These global random unitaries can be generated in interacting quantum lattice models with engineered disorder using random quenches [17, 28, 29] and the corresponding protocols are in particular relevant for atomic Hubbard models [17, 29].

In the second part, we extend the formalism to derive a protocol to measure the overlap $\mathrm{Tr}\left[\rho\rho'\right]$ of two states ρ and ρ' which are prepared sequentially in an experiment. This allows in particular to directly measure the many-body Loschmidt echo [30], without implementing time-reversed operations. Finally, we discuss within our formalism a proposal of Ohliger et al. [31] to use randomized measurements, implemented with global random unitaries, to perform full quantum state tomography in atomic Hubbard models. We generalize this protocol to local random unitaries available in spin models and investigate in detail numerically how the required number of measurements to reconstruct the density matrix ρ up to a fixed error scales with system size.

[*] andreas.elben@uibk.ac.at

II. MEASUREMENT OF THE SECOND RÉNYI ENTROPY

In this section, we discuss the measurement of the second Rényi entropy in quantum lattice models. After a short review, we focus on protocols utilizing randomized measurements, give explicit recipes and discuss examples. We consider a lattice system $\mathcal{S}$ described by a quantum state ρ. The second Rényi entropy $S_2(\rho_A)$ of the reduced density matrix $\rho_A = \mathrm{Tr}_{\mathcal{S}\setminus A}\left[\rho\right]$ of an arbitrary subsystem $A \subseteq \mathcal{S}$ consisting of N_A sites is defined as

$$S_2(\rho_A) = -\log_2 \mathrm{Tr}\left[\rho_A^2\right]. \qquad (1)$$

Using $S_2(\rho_A)$, one shows that bipartite entanglement exists between two disjoint subsystems A and B of $\mathcal{S}$ with reduced density matrices $\rho_A = \mathrm{Tr}_{\mathcal{S}\setminus A}\left[\rho\right]$ and $\rho_B = \mathrm{Tr}_{\mathcal{S}\setminus B}\left[\rho\right]$ [32] if

$$\begin{aligned} &S_2\left(\rho_A^2\right) > S_2\left(\rho_{A\cup B}^2\right) \\ \text{and}\quad &S_2\left(\rho_B^2\right) > S_2\left(\rho_{A\cup B}^2\right), \end{aligned} \qquad (2)$$

where $\rho_{A\cup B} = \mathrm{Tr}_{\mathcal{S}\setminus A\cup B}\left[\rho\right]$ is the reduced density matrix of $A \cup B$ [6].

To measure $S_2(\rho_A)$, i.e. the purity $\mathrm{Tr}\left[\rho_A^2\right]$ of a (reduced) density matrix ρ_A, various protocols have proposed and realized which we shortly review in the following: A first option realized in spin models is to perform full quantum state tomography of ρ_A [7–10]. However, due to the exponential scaling of the number measurement settings, at least d^{2N_A} for N_A spins and standard tomography [8], this approach is limited to system with a few degrees of freedom [7]. On the contrary, recent efficient tomographic methods require a specific structure of the state of interest [9, 10].

A second class of protocols [14, 15] is based on noting that the purity

$$\mathrm{Tr}\left[\rho_A^2\right] = \mathrm{Tr}\left[\mathbb{S}\rho_A \otimes \rho_A\right] \qquad (3)$$

can be obtained from measuring the expectation value of the swap operator $\mathbb{S}$ acting on two copies of a quantum state ρ_A [13, 33]. Here, $\mathbb{S}$ is defined by $\mathbb{S}\left|s_A\right\rangle \otimes \left|s'_A\right\rangle = \left|s'_A\right\rangle \otimes \left|s_A\right\rangle$ for any two states $\left|s_A\right\rangle, \left|s'_A\right\rangle$. Prerequisite for these protocols is thus the experimental ability to create two identical copies $\rho_A \otimes \rho_A$ and to perform joint operations on them to measure $\mathrm{Tr}\left[\mathbb{S}\rho_A \otimes \rho_A\right] = \mathrm{Tr}\left[\rho_A^2\right]$. Despite the experimental complexity of this task, the purity of a quantum state of up to six particles, realizing a one-dimensional Bose-Hubbard model, has been measured in remarkable experiments [11, 12]. Recently, the method has been also transferred to trapped-ion quantum simulator, and applied to a one-dimensional system of five qubits [34]. Creating identical copies of a quantum state in larger systems and higher spatial dimensions remains however a significant technological challenge.

Only a single instance of a quantum state is required in a third class of protocols [16, 17, 27, 29], utilizing statistical correlations of randomized measurements, which we discuss in the remainder of this paper.

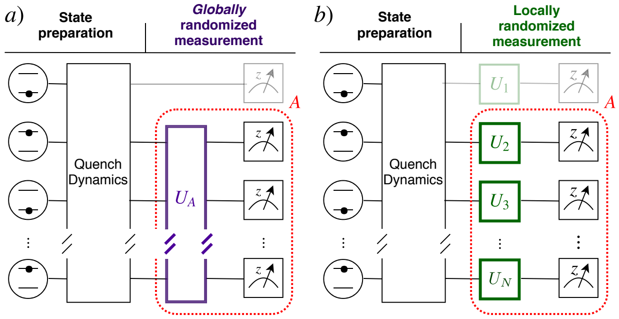

FIG. 1. *Measurement of the second Rényi entropy using statistical correlation between randomized measurements.* A quantum state ρ of interest is prepared for instance via quench dynamics (see also Ref. [16]). A randomized measurement on a subsystem A is performed by the application of a) a global random unitary U_A from a unitary 2-design on the entire Hilbert space or b) a product of local random unitaries $U_A = \bigotimes_{i\in A} U_i$ sampled independently from a unitary 2-design on $\mathfrak{h}$. Subsequently, a measurement in the computational basis is performed. From statistical correlations of the outcomes of such randomized measurements, the purity $\mathrm{Tr}\left[\rho_A^2\right]$ of the reduced density matrix ρ_A is estimated (see text).

A. Second Rényi entropy from statistical correlations of randomized measurements

In this subsection, we describe the protocol to estimate the purity $\mathrm{Tr}\left[\rho_A^2\right]$ of a (reduced) density matrix ρ_A from statistical correlation of randomized measurements. While protocols based on global random unitaries are also applicable to atomic Hubbard models [17, 29], we focus in this paper on spin models consisting of N spins with local Hilbert space $\mathfrak{h}$ of dimension d (i.e. N qudits). Here, in addition, experimentally simpler local random unitaries are available (see below). A schematic view of the experimental sequence we have in mind is displayed in Fig. 1 (see also Ref. [16, 17]). An (entangled) quantum state of interest ρ is for instance prepared via quench dynamics originating from a simple initial state. The experimental protocol to measure the purity of the reduced density matrix ρ_A of a subsystem A of N_A qudits consists then in several steps. First, one applies to ρ_A a random unitary U_A. This can (i) either be a *global* random unitary sampled from a unitary 2-design [35] defined on the entire Hilbert space $\mathcal{H}_A = \mathfrak{h}^{\otimes N_A}$ with dimension $\mathcal{D}_A = d^{N_A}$ of the subsystem, or (ii) a *local* unitary of the form $U = \bigotimes_{i\in A} U_i$ where the U_i are sampled independently from a unitary 2-design defined on the local Hilbert space $\mathfrak{h}$. We compare both approaches in detail below. Subsequently, a measurement in the computational basis is performed. This is repeated with the same random unitary U_A to estimate the occupation probabilities $P_U(\mathbf{s}_A) = \mathrm{Tr}\left[U_A \rho U_A^\dagger \left|\mathbf{s}_A\right\rangle\left\langle\mathbf{s}_A\right|\right]$ of computational basis states $\left|\mathbf{s}_A\right\rangle = \left|s_1, \ldots, s_{N_A}\right\rangle$ ($s_i = 1 \ldots d$ for $i \in A$). In a second step, this is repeated for many different random unitaries, to estimate the average over the ensemble of random unitaries.

Given the set of outcome probabilities $P_U(\mathbf{s}_A)$ for the computational basis states $\mathbf{s}_A$, one estimates the purity of ρ_A from second-order cross correlations across the random unitary ensemble. For *global* random unitaries [case (i)], one finds

$$\begin{aligned}\operatorname{Tr}\left[\rho_A^2\right] &= \mathcal{D}_A \sum_{\mathbf{s}_A,\mathbf{s}'_A} (-\mathcal{D}_A)^{-D_G[\mathbf{s}_A,\mathbf{s}'_A]}\, \overline{P_U(\mathbf{s}_A)P_U(\mathbf{s}'_A)} \\ &= (\mathcal{D}_A+1)\sum_{\mathbf{s}} \overline{P_U(\mathbf{s}_A)^2} - 1, \qquad (4)\end{aligned}$$

where the "global" Hamming distance is defined as $D_G[\mathbf{s}_A,\mathbf{s}'_A] = 1$ if $\mathbf{s}_A = \mathbf{s}'_A$ and $D_G[\mathbf{s}_A,\mathbf{s}'_A] = 1$ if $\mathbf{s}_A \neq \mathbf{s}'_A$. The expression in the second line has first been given in Ref. [27]. If independent *local* random unitaries on individual qudits are used [case (ii)], the purity is estimated from

$$\operatorname{Tr}\left[\rho_A^2\right] = d^{N_A} \sum_{\mathbf{s}_A,\mathbf{s}'_A} (-d)^{-D[\mathbf{s}_A,\mathbf{s}'_A]}\, \overline{P_U(\mathbf{s}_A)P_U(\mathbf{s}'_A)}, \qquad (5)$$

where the Hamming distance $D[\mathbf{s}_A,\mathbf{s}'_A]$ between two states $|\mathbf{s}_A\rangle = |s_1,\dots,s_{N_A}\rangle$ and $|\mathbf{s}'_A\rangle = |s'_1,\dots,s'_{N_A}\rangle$ is defined as the number of local constituents $i \in A$ where $s_i \neq s'_i$, i.e. $D[\mathbf{s}_A,\mathbf{s}_A'] \equiv \#\{i \in A \,|\, s_i \neq s'_i\}$. Equation (5) has first been obtained and proved by direct calculation in Ref. [16], and represents an explicit version of the recursive formula given in Ref. [17]. It is the aim of the present paper to give an in depth derivation of Eq. (5) by developing a general formalism to evaluate statistical correlations of randomized measurements.

An intriguing connection to the previous works realizing the swap operator on two *physical copies* [11, 12, 14, 15] can be seen as follows: We can rewrite any product of outcome probabilities $P_U(\mathbf{s}_A)P_U(\mathbf{s}'_A) = \operatorname{Tr}_{\mathcal{H}_A^{\otimes 2}}\left[U_A^{\otimes}\rho_A^{\otimes 2}U_A^{\dagger\otimes 2}\,|\mathbf{s}_A\rangle\langle\mathbf{s}_A| \otimes |\mathbf{s}'_A\rangle\langle\mathbf{s}'_A|\right]$ as the expectation value of an operator $|\mathbf{s}_A\rangle\langle\mathbf{s}_A| \otimes |\mathbf{s}'_A\rangle\langle\mathbf{s}'_A|$ on the doubled Hilbert space $\mathcal{H}_A^{\otimes 2}$. We can thus intuitively understand the ensemble average over second order cross correlations taken in Eqs. (4) and (5) as an effective construction of the swap operator on two *virtual copies* of ρ_A (see for details Sec. III).

The approaches with global and local random unitaries differ in various aspects: First, the implementation of global random unitaries from a unitary 2-design acting on the entire many-body quantum state ρ_A requires interactions between the particles. It has been proposed to prepare them efficiently in quantum circuits using (random) entangling gates [36] or in generic interacting many-body systems using time evolution subject to random quenches [17, 28, 29, 31]. On the contrary, local random unitaries, available in spin models, are single "qudit" operations (random spin rotations) which have been demonstrated with high fidelity and repetition rate [16]. Second, the protocol utilizing local random unitaries allows, from a single experimental dataset obtained from randomized measurements on the subsystem A, to estimate the purity $\operatorname{Tr}\left[\rho_{A'}^2\right]$ of the reduced density matrix $\rho_{A'}$ of any subsystem $A' \in A$. To this end, Eq. (5) is evaluated with occupation probabilities $P_U(\mathbf{s}_{A'})$ of states $|\mathbf{s}_{A'}\rangle$ of the logical basis of A'. Third, the two protocols differ in their sensitivity to statistical errors. In an experiment, statistical errors of the estimated purity arise from a finite number N_U of applied unitaries and a finite number N_M of measurements per random unitary (projection noise). The total number of measurements $N_M N_U$ scales exponentially with the number N_A of degrees of freedom in the subsystem A, with exponents significantly smaller than in full quantum state tomography [16, 17]. As we discuss in detail below, the protocol utilizing global unitaries is, for pure product states, favorable in terms of statistical errors.

To prove Eqs. (4) and (5), we introduce results of the theory of random unitaries in Sec. III. The proof follows then in Sec. IV A.

B. Illustrative examples

In the remainder of this section, we illustrate Eqs. (4) and (5) using simple examples.

1. Single qubit

The density matrix $\rho = \frac{1}{2}\left(\mathbb{1}_2 + \mathbf{v}\cdot\sigma\right)$ of a single qubit is conveniently represented on the Bloch sphere, with the real Bloch vector $(\mathbf{v})_i = \operatorname{Tr}[\rho\sigma_i]$ and $\sigma = (\sigma_x,\sigma_y,\sigma_z)$ the Pauli matrices. The purity $\operatorname{Tr}\left[\rho^2\right] = \frac{1}{2}\left(1+|\mathbf{v}|^2\right)$ is thus fully determined by the length of the Bloch vector $|\mathbf{v}|$. Our approach to estimate the length of the Bloch vector consists in applying a random unitary U to the state ρ and measuring the difference of occupation $Z_U = P_U(\uparrow) - P_U(\downarrow) = \operatorname{Tr}\left[U\rho U^\dagger\sigma_z\right] = (Q_U\mathbf{v})_3$ of the computational basis states $|\uparrow\rangle, |\downarrow\rangle$. Here, Q_U is the unique rotation matrix corresponding the unitary U, i.e. $U\mathbf{v}\cdot\sigma U^\dagger = (Q_U\mathbf{v})\cdot\sigma$ for all Bloch vectors $\mathbf{v}$ [37]. This is now repeated with different random unitaries, to sample the distribution of Z_U across the circular unitary ensemble. Since the distribution of $Z_U = (Q_U\mathbf{v})_3$ describes the z-component of the rotated Bloch vector $Q_U\mathbf{v}$ subject to arbitrary rotations Q_U, it is intuitively apparent that it contains information about the length of $\mathbf{v}$ (see also Fig. 2).

Formally, we note that moments $\overline{Z_U^n}$ ($n \in \mathbb{N}$) of the random variable Z_U are invariant under unitary transformations due to the invariance properties of the Haar measure [see below, Eq. (14)]. Thus, they must be determined by properties of the Bloch vector $\mathbf{v}$ which are invariant under arbitrary rotations. The squared length $|\mathbf{v}|^2$ is its unique second order invariant, and thus we conclude $\overline{Z_U^2} = \overline{(Q_U\mathbf{v})_3^2} \sim |\mathbf{v}|^2$. Indeed, by explicit calculation, we find that Z_U is uniformly distributed,

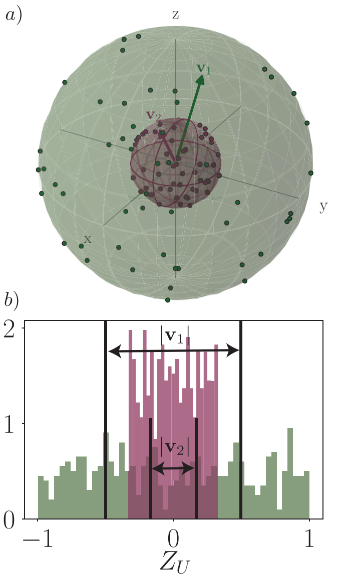

FIG. 2. a) Graphical visualization of a pure ρ_1 (green) and a mixed ρ_1 (purple) singe single qubit state with Bloch vectors (arrows) $\mathbf{v}_1$ and $\mathbf{v}_2$, respectively. Points correspond to 50 randomly rotated states, generated via the application of random unitaries sampled from the CUE [38] to ρ_1 and ρ_2, respectively. b) Histogram of the random variable $Z_U = \mathrm{Tr}\left[U\rho U^\dagger\sigma_z\right]$ for pure ρ_1 (green) and mixed ρ_2 (purple) state, the indicated standard deviation (multiplied with a factor $\sqrt{3}$) corresponds to the length of the Bloch vectors.

with zero mean and variance $\overline{Z_U^2} = |\mathbf{v}|^2/3$, such that $\mathrm{Tr}\left[\rho^2\right] = \frac{1}{2}\left(1 + 3\overline{(P_U(\uparrow) - P_U(\downarrow))^2}\right)$. Inserting that $1 = (P_U(\uparrow) + P_U(\downarrow))^2$ we can bring this into a more symmetric form to arrive at

$$\mathrm{Tr}\left[\rho^2\right] = 2\left(\overline{P_U(\uparrow)^2 + P_U(\downarrow)^2 - P_U(\uparrow)P_U(\downarrow)}\right) \tag{6}$$

which corresponds to Eq. (4) [Eq. (5)] for the special case of $\mathcal{D}_A = 2$ [$d = 2$ and $N_A = 1$].

2. *Two qubits*

We consider now the case of two qubits where randomized measurements are implemented using independent local random unitaries $U = U_1 \otimes U_2$. Generalizing the single-qubit case, the two-qubit system is conveniently represented in the basis of Pauli strings

$$\rho = \frac{1}{4}\sum_{\mu,\nu=0}^{3} r_{\mu\nu}\;\sigma_\mu \otimes \sigma_\nu, \tag{7}$$

where $\sigma_0 = \mathbb{1}_2$ and σ_i the Pauli matrices ($1 \le i \le 3$). The real coefficients $r_{\mu\nu} = \mathrm{Tr}\left[\rho\sigma_\mu \otimes \sigma_\nu\right]$ constitute the Bloch matrix $\mathbf{r}$ (generalizing the Bloch vector)

$$r = \left(\begin{array}{c|ccc} 1 & r_{01} & r_{02} & r_{03} \\ \hline r_{10} & r_{11} & r_{12} & r_{13} \\ r_{20} & r_{21} & r_{22} & r_{23} \\ r_{30} & r_{31} & r_{32} & r_{33} \end{array}\right) \equiv \begin{pmatrix} 1 & \mathbf{v}^\dagger \\ \mathbf{u} & R \end{pmatrix}, \tag{8}$$

where $u_i = r_{i0}$, $v_j = r_{0j}$, and $R_{ij} = r_{ij}$. The vectors $\mathbf{u}$ and $\mathbf{v}$ are the Bloch vectors of the reduced density matrices $\rho_1 = \mathrm{Tr}_2\left[\rho\right]$ and $\rho_2 = \mathrm{Tr}_1\left[\rho\right]$ of the individual qubits, respectively. The matrix R quantifies the correlations between the two qubits [37]. Using these definitions, the purity of the density matrix ρ is then given by

$$\mathrm{Tr}\left[\rho^2\right] = \frac{1}{4}\left(1 + |\mathbf{u}|^2 + |\mathbf{v}|^2 + ||R||^2\right), \tag{9}$$

where $||R||^2 = \mathrm{Tr}\left[R^\dagger R\right]$.

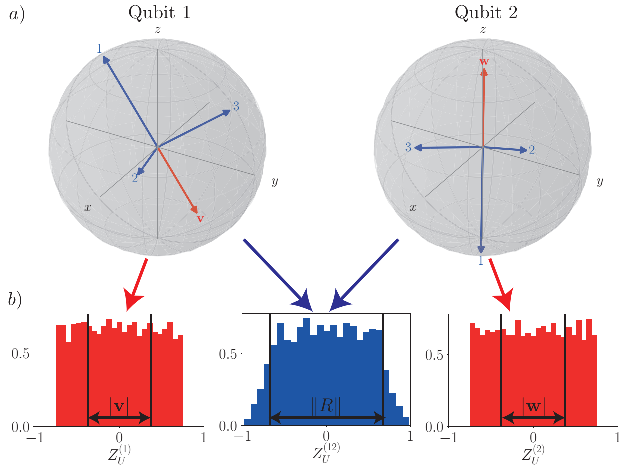

FIG. 3. a) Graphical visualization of a pure, random (entangled) two-qubit state using. The red arrows visualize the Bloch vectors $\mathbf{v}$ and $\mathbf{w}$ of reduced (mixed) single qubit states. Blue arrows correspond to the left $\sqrt{\gamma_i}\mathbf{m}_i$ and right $\sqrt{\gamma_i}\mathbf{n}_i$ singular vectors, rescaled with singular values γ_i, of the singular value decomposition of R ($i = 1, \ldots, 3$) [37]. The measurement of $\sigma_z \otimes \sigma_z$ after the application of a unitary $U_1 \otimes U_2$ (rotations Q_1 and Q_2 of qubit 1 and 2) is visualized as a projection of the singular vectors onto the z-axis, its expectation value is given as $\sum_i \gamma_i (Q_1\mathbf{m}_i)_3 (Q_2\mathbf{n}_i)_3$. b) Histograms of random variables $Z_U^{(1)} = \mathrm{Tr}\left[U\rho U^\dagger \sigma_z \otimes \mathbb{1}_2\right]$, $Z_U^{(2)} = \mathrm{Tr}\left[U\rho U^\dagger \mathbb{1}_2 \otimes \sigma_z\right]$ and $Z_U^{(12)} = \mathrm{Tr}\left[U\rho U^\dagger \sigma_z \otimes \sigma_z\right]$ generated using random unitaries of the form $U = U_1 \otimes U_2$. The standard deviation corresponds to the length of the Bloch vectors $|\mathbf{v}|$ and $|\mathbf{w}|$ (left and right) and the Hilbert-Schmidt norm $||R||$ of the correlation matrix R (middle), see text.

Our aim is to estimate the purity $\mathrm{Tr}\left[\rho^2\right]$ using random unitaries of the $U_1 \otimes U_2$ and (collective) measurements in the computational basis $|\uparrow\uparrow\rangle, |\uparrow\downarrow\rangle, |\downarrow\uparrow\rangle, |\downarrow\downarrow\rangle$. First, we note that under unitary transformation $\rho \to U_1 \otimes U_2 \rho U_1^\dagger \otimes U_2^\dagger$, the individual elements of the Bloch matrix transform as

$$\begin{aligned} \mathbf{v} &\rightarrow \mathbf{v}' = Q_1 \mathbf{v} \\ \mathbf{w} &\rightarrow \mathbf{w}' = Q_2 \mathbf{w} \\ R &\rightarrow R' = Q_1 R Q_2^\dagger, \end{aligned} \tag{10}$$

there Q_1 (Q_2) is the unique rotation matrix corresponding to U_1 (U_2) [37]. Thus $|u|^2$ and $|v|^2$ can be estimated from single qubit measurements, i.e. from the variances of the distributions

$$\begin{aligned} Z_U^{(1)} &= P_U^{(1)}(\uparrow) - P_U^{(1)}(\downarrow) \\ &= P_U(\uparrow\uparrow) + P_U(\uparrow\downarrow) - P_U(\downarrow\uparrow) - P_U(\downarrow\downarrow) \end{aligned} \tag{11}$$

and $Z_U^{(2)}$, respectively. The unique element of the (transformed) correlation matrix accessible from measurements solely in the computational basis is

$$\begin{aligned} Z_U^{(1,2)} &= \mathrm{Tr}\left[U_1 \otimes U_2 \rho U_1^\dagger \otimes U_2^\dagger \sigma_z \otimes \sigma_z\right] \\ &= P_U(\uparrow\uparrow) - P_U(\uparrow\downarrow) - P_U(\downarrow\uparrow) + P_U(\downarrow\downarrow) \\ &= \left(Q_1 R Q_2^\dagger\right)_{33}. \end{aligned} \tag{12}$$

Again, due to the Haar average, moments of the random variable $Z_U^{(1,2)}$ must be invariant transformations (10) with arbitrary rotations Q_1 and Q_2, and a second order invariant of this type is the matrix norm $||R||_2$. Indeed, we find $\overline{\left(Z_U^{(1,2)}\right)^2} = ||R||_2/9$. Thus we obtain,

$$\begin{aligned} \mathrm{Tr}\left[\rho^2\right] &= \frac{1}{4}\left(1 + 3\overline{\left(Z_U^{(1)}\right)^2} + 3\overline{\left(Z_U^{(2)}\right)^2} + 9\overline{\left(Z_U^{(1,2)}\right)^2}\right) \\ &= 4 \sum_{\substack{\mathbf{s},\mathbf{s}'= \\ \uparrow\uparrow,\uparrow\downarrow,\downarrow\uparrow,\downarrow\downarrow}} (-2)^{-D[\mathbf{s},\mathbf{s}']} \overline{P_U(\mathbf{s}) P_U(\mathbf{s}')}, \end{aligned} \tag{13}$$

which corresponds to formula (5) for the special case of $d = 2$ and $N_A = 2$. To arrive at the last line, we used that $1 = (P_U(\uparrow\uparrow) + P_U(\uparrow\downarrow) + P_U(\downarrow\uparrow) + P_U(\downarrow\downarrow))^2$. We note that these arguments generalize to N_A-qubit systems whose density matrix can be parametrized by a rank N_A "Bloch tensor". The second moment of a suitably generalized random variable $Z_U^{(1,\ldots,N_A)} = \mathrm{Tr}\left[\bigotimes_{i=1}^{N_A} U_i \rho \bigotimes_{i=1}^{N_A} U_i^\dagger \sigma_z^{\otimes N_A}\right]$ is connected to the Hilbert-Schmidt norm $||R^{(N_A)}||^2$ of the rank N_A "correlation tensor" $R^{(N_A)}$.

III. RANDOM UNITARIES, DIAGRAMMATIC CALCULUS AND UNITARY k-DESIGNS

In this section, we provide an overview over the mathematical tools necessary to describe randomized measurements based on random unitaries. We consider first a single qudit with Hilbert space $\mathscr{h}$ of (arbitrary) dimension d, which also to corresponds to the case of global random unitaries (with the replacement $\mathscr{h} \rightarrow \mathcal{H}_A$, $d \rightarrow \mathcal{D}_A = d^{N_A}$, see Sec. II A). In this setting, we introduce the Haar measure, defining the CUE, and derive elementary properties of the unitary twirling channel. Moreover, we introduce a graphical calculus simplifying the calculations. In the last subsection, we extend the framework to composite systems of many qudits where multiple, independent, random unitaries are applied locally.

A. Haar randomness

We first provide an overview over Haar random unitaries and introduce the central object of our formalism, the unitary twirling channel. We follow the treatment of Ref. [39]. An orthonormal basis of $\mathscr{h}$ is denoted with $\{|s\rangle\}$.

The most important ingredient are Haar random unitaries. These are unitary matrices which are distributed according to the probability distribution defined by the Haar measure on the unitary group [40]. Here, the Haar measure is the unique probability measure on the group of unitary matrices $\mathcal{U}(\mathscr{h})$ on $\mathscr{h}$ which is both left- and right- invariant, i.e. it satisfies for any function f on $\mathcal{U}(\mathscr{h})$ and any unitary $V \in \mathcal{U}(\mathscr{h})$

$$\begin{aligned} &\int_{\mathrm{Haar}} \mathrm{d}U = 1, \\ &\int_{\mathrm{Haar}} \mathrm{d}U f(VU) = \int_{\mathrm{Haar}} \mathrm{d}U f(UV) = \int_{\mathrm{Haar}} \mathrm{d}U f(U) \ . \end{aligned} \tag{14}$$

Often, $\mathcal{U}(\mathscr{h})$ equipped with the Haar measure is also called the *circular unitary ensemble* (CUE) [41], and we use $\overline{f(U)} \equiv \int \mathrm{d}U f(U)$ to denote the ensemble average over the CUE.

In the following, we consider the k-fold copy space $\mathscr{h}^{\otimes k}$, $k \in \mathbb{N}$, to calculate higher order moments of random unitaries. We note that this is a purely mathematical construction: kth-order products of outcome probabilities of randomized measurements can be viewed as expectation value an operator acting on $\mathscr{h}^{\otimes k}$, realizing thus k "virtual copies". On the contrary, it is a key property of any measurement protocol presented in this paper that only *a single physical instance* of a quantum state is required in the experiment. We define on $\mathscr{h}^{\otimes k}$ a quantum channel, the k-fold twirl by

$$\Phi^{(k)}(O) = \int_{\mathrm{Haar}} \mathrm{d}U \left(U^\dagger\right)^{\otimes k} O U^{\otimes k}. \tag{15}$$

for any operator O on $\mathscr{h}^{\otimes k}$. As a simple consequence of the invariance of the Haar measure [Eq. (14)], $\Phi^{(k)}$ forms a projector $\Phi^{(k)}(\Phi^{(k)}(O)) = \Phi^{(k)}(O)$. We show in the following that its image is spanned by permutation operators W_π , for permutations $\pi = (\pi(1), \ldots, \pi(k)) \in \mathcal{S}_k$ with the symmetric group $\mathcal{S}_k$, which are defined as

$$W_\pi = \sum_{s_1,\ldots,s_k=1}^{d} |s_{\pi(1)}\rangle \cdots |s_{\pi(k)}\rangle \langle s_1| \cdots \langle s_k| \ . \tag{16}$$

These operators permute states between individual copies $W_\pi |s_1\rangle \cdots |s_k\rangle = |s_{\pi(1)}\rangle \cdots |s_{\pi(k)}\rangle$. Using that $[W_\pi, V^{\otimes k}] = 0$ for any $\pi \in \mathcal{S}_k$, it follows directly that $\Phi^{(k)}(W_\pi) = W_\pi$, i.e. the permutation operators W_π are invariant under the projection $\Phi^{(k)}$. Indeed, they span the total image of $\Phi^{(k)}$, which is proved with the Schur Weyl duality [39]. Explicitly, one finds

$$\Phi^{(k)}(O) = \sum_{\pi,\sigma \in \mathcal{S}_k} C_{\pi,\sigma} \operatorname{Tr}\left[W_\sigma O\right] W_\pi, \tag{17}$$

where the coefficients $C_{\pi,\sigma} = \mathrm{Wg}(\pi\sigma^{-1})$ constitute the real-valued, symmetric Weingarten matrix C determined by the Weingarten function Wg [39, 42, 43]. For $k \leq d$, C is invertible, with inverse $Q \equiv C^{-1}$ and $Q_{\pi,\sigma} = d^{\sharp\mathrm{cycles}(\pi\sigma)}$ [39]. For $k = 1$ and $k = 2$, we find

$$\Phi^{(1)}(O) = \frac{\mathbb{1}}{d} \operatorname{Tr}\left[O\right] \tag{18}$$

and

$$\begin{aligned}\Phi^{(2)}(O) = \frac{1}{d^2 - 1} \Bigg(& \mathbb{1} \operatorname{Tr}\left[O\right] + \mathbb{S} \operatorname{Tr}\left[\mathbb{S} O\right] \\ & - \frac{1}{d} \mathbb{S} \operatorname{Tr}\left[O\right] - \frac{1}{d} \mathbb{1} \operatorname{Tr}\left[\mathbb{S} O\right] \Bigg),\end{aligned} \tag{19}$$

with the identity $\mathbb{1} = W_{(1)(2)}$ and $\mathbb{S} = W_{(1,2)} = \sum_{s_1 s_2} |s_2\rangle |s_1\rangle \langle s_1| \langle s_2|$ being the swap operator.

B. Diagrammatic calculus

In the previous section, we showed how to evaluate the unitary twirling channel $\Phi^{(k)}$ in terms of permutation operators. Here, we introduce a graphical calculus which enables the evaluation of arbitrary functionals of random unitaries, in particular $\Phi^{(k)}$. We follow and adapt here the treatment of Ref. [42] (see also Ref. [44] for a similar approach). We first note that, for any $k \in \mathbb{N}$, an operator O acting on $\mathcal{H}^{\otimes k}$ can be viewed as a (k,k)-tensor $O \in \mathcal{H}^{*\otimes k} \otimes \mathcal{H}^{\otimes k}$ with k covariant and k contravariant indices. As shown in Fig. 4(a), we represent tensors in the following as a box with decorations, where the number of empty (filled) symbols corresponds to the number of contravariant (covariant) indices. Similarly, ket vectors $|a\rangle \in \mathcal{H}$ can be viewed as a $(0,1)$ tensors with a single white decoration, and bra vectors $\langle a| \in \mathcal{H}^*$ are $(1,0)$ tensors with a single black decoration. As discussed in the previous section, permutation operators are of central importance to evaluate twirling channels. Thus, we introduce a special graphical notation displayed in Fig. 4(b), which corresponds directly to their action on the k-fold copy space.

In order evaluate the Haar average of an arbitrary diagram containing random unitaries, it turns out to be useful to consider Bell states $\sum_i |i\rangle |i\rangle$ [$\sum_i \langle i| \langle i|$], which represent special $(0,2)$ [$(2,0)$] tensors [Fig. 5(a)]. These allow the definition of graphs connecting two decorations of identical color [Fig. 5(b)] and, using the identity $(O^T)_{ij} = O_{ji} = \sum_{k,k'} \langle i|k\rangle \langle k'|O|k\rangle \langle k'|j\rangle$, the transposed matrix, given as the tensor with interchanged decorations [Fig. 5(c)].

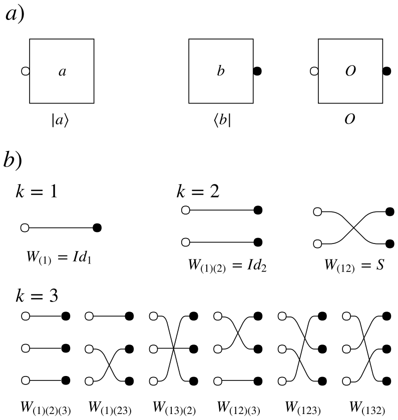

FIG. 4. Graphical dictionary: a) Elementary diagrams, describing ket-vectors [(0,1)-tensors], bra-vectors [(1,0)-tensors] and operators [(1,1)-tensors] on a single copy. b) Graphical representation of permutation operators [(k,k)-tensors] acting on the k-fold copy space.

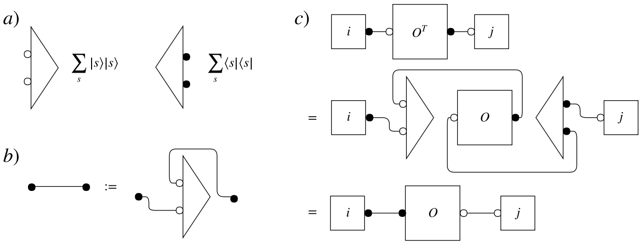

FIG. 5. Bell states and the transpose matrix: a) Definition of Bell states [(0,2)- and (2,0)-tensor] on two copies. b) Definition of a diagram connecting two decorations of the same color, in the analogous way the diagram connecting to white decorations is defined. c) Visualization of the transposed matrix using Bell states (see text).

Equipped with this definitions, we are now in the position to evaluate the ensemble average of an arbitrary diagram. We describe a general procedure [42] applicable to any diagram. As an explicit example we present in Fig. 6 the evaluation of $\langle i| \langle j| \Phi^{(2)}(U) |i'\rangle |j'\rangle$ [45]. The first step is to replace all unitaries U^T with U and $U^\dagger$ with U^* using the Bell states and tensors defined in Fig. 5. If in the resulting diagram, the number of unitaries U does not equal the number of complex conjugates U^*, the diagram evaluates to zero. Otherwise, white decorations of boxes U are connected with white decorations of boxes U^* and black decorations of boxes U are (independently) connected with black of boxes U^*. Subsequently decorations and boxes of the random unitaries are removed. Given k boxes U, there exist $(k!)^2$ possible ways to draw these connections. The ensemble average is obtained as a

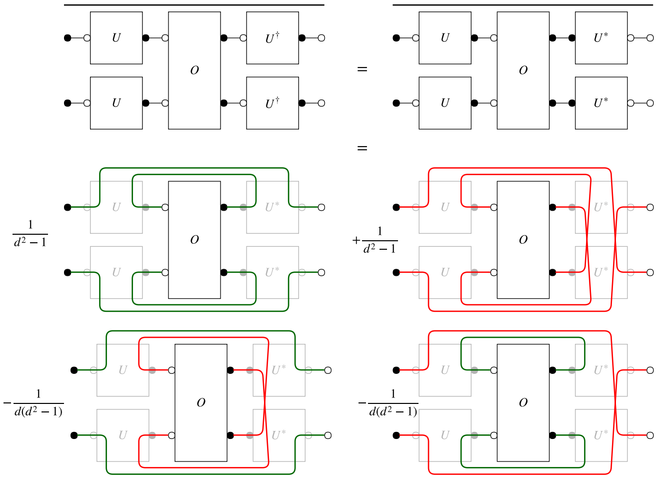

FIG. 6. Graphical evaluation of $\Phi^{(2)}$. We evaluate graphical the matrix element $\langle i| \langle j| \Phi^{(2)}(O) |i'\rangle |j'\rangle$. For clarity the boxes describing the basis states $\langle i| \langle j|$, $|i'\rangle |j'\rangle$ have been omitted, only their decorations are kept.

weighted sum of all resulting diagrams, with coefficients determined by the Weingarten matrix. To calculate these coefficients, one labels both the boxes U and boxes U^* with arbitrary integers $1, \dots k$. Each possibility to connect white (black) decorations is now described by a permutation $\alpha \in S_k$ ($\beta \in S_k$): If the white decoration of U-box i is connected to the white decoration of U^*-box j, then $\alpha(i) \equiv j$. The coefficient of a diagram is obtained as $\mathrm{Wg}(\alpha\beta^{-1})$. In the case of Fig. 6, there exist four possibilities, and the resulting sum of diagrams is the graphical representation Eq. (19).

C. Unitary k-designs

In the previous sections, we considered Haar random unitaries drawn from the circular ensemble for which Eq. (17) holds for arbitrary $k \in \mathbb{N}$. In applications, one is however typically interested in moments of random unitaries up to a finite (small) number k [28], for instance $k = 2$ for the estimation of second order Rényi entropy. Since the preparation of Haar random unitaries using, for instance, random quantum circuits requires an amount of resources scaling exponentially with system size [28], simpler ensembles, unitary k-designs, have been introduced [35, 36, 46]. These ensembles approximate Haar random unitaries in the sense that up to k-th order moments are identical, i.e. Eq. (17) holds, for an arbitrary operator O, up to a finite, fixed k [47]. To define unitary k-designs formally, we introduce the k-fold twirl with respect to a continuous ensemble $\mathcal{E}$ of unitary operators by

$$\Phi^{(k)}_{\mathcal{E}}(O) = \int_{\mathcal{E}} \mathrm{d}U \, \left(U^\dagger\right)^{\otimes k} O U^{\otimes k}, \tag{20}$$

and for a discrete ensemble $\mathcal{E}$ with cardinality $|\mathcal{E}|$ by

$$\Phi^{(k)}_{\mathcal{E}}(O) = \frac{1}{|\mathcal{E}|} \sum_{U \in \mathcal{E}} \left(U^\dagger\right)^{\otimes k} O U^{\otimes k}. \tag{21}$$

One says that $\mathcal{E}$ forms an *unitary k-design* if and only if $\Phi^{(k)}_{\mathcal{E}} = \Phi^{(k)}$ and that $\mathcal{E}$ forms an *ϵ-approximate k-design* if and only if $||\Phi^{(k)}_{\mathcal{E}} - \Phi^{(k)}||_\diamond < \epsilon$ [36]. It follows directly that any k-design is also an k' design, for any $k' < k$. A prime example of an exact 3-design is the Clifford group [46]. Importantly, ϵ-approximate k-design can be prepared efficiently in local random quantum circuits [36], and generic interacting quantum simulators [17, 28, 29].

D. Composite systems

In this section, we generalize our treatment to composite systems consisting of N_A qudits with Hilbert space $\mathcal{H} = \hbar^{\otimes N_A}$. For simplicity of notation we drop the subscript A. The basis $\{|\mathbf{s}\rangle\}$ denotes a product basis $|\mathbf{s}\rangle = \otimes_{i=1}^N |s_i\rangle$ for all $\mathbf{s} = (s_1, \dots, s_N)$. We consider random unitaries of the form $U = \bigotimes_{i=1}^N U_i$ where the U_i ($i \in \{1, \dots, N\}$), acting on the individual qudits, are sampled independently from the CUE($\hbar$) (a unitary k-design) defined on the local Hilbert space $\hbar$. We define a k-fold local twirling channel by

$$\Phi^{(k)}_N(O) \equiv \overline{\left(U^{\otimes k}\right)^\dagger O U^{\otimes k}}, \tag{22}$$

where $\overline{\dots}$ denotes in this context the ensemble average over random unitaries of the form $U = \bigotimes_{i=1}^N U_i$. Generalizing Eq. (17), we find

$$\Phi^{(k)}_N(O) = \sum_{\pi, \sigma \in \mathcal{S}_k^{\otimes N}} C_{\pi,\sigma} W_\pi \mathrm{Tr}\left[W_\sigma O\right]. \tag{23}$$

Here, $\pi = \bigotimes_{i=1}^N \pi_i \in \mathcal{S}_k^{\otimes N}$ and $\sigma = \bigotimes_{i=1}^N \sigma \in \mathcal{S}_k^{\otimes N}$ are tensor products of permutations and the corresponding operators $W_\pi \equiv \bigotimes W_{\pi_i}$ act locally on the k-fold copy space $\hbar^{\otimes k}$ of the individual qubits. The coefficients $C_{\pi,\sigma} \equiv \prod_{i=1}^N C_{\pi_i,\sigma_i}$ are determined by products of elements of the Weingarten matrix C. To proof Eq. (23), we first note that we can expand an arbitrary operator O in a product basis of the N qudits $O = \sum_\alpha c_\alpha O_{\alpha_1} \otimes \dots \otimes O_{\alpha_N}$. By linearity, it suffices thus to restrict to O being a tensor product of local operators, i.e. $O = \bigotimes_{i=1}^N O_i$. We find

$$\begin{aligned}
\Phi^{(k)}_N\left(\bigotimes_{i=1}^N O_i\right) &= \bigotimes_{i=1}^N \overline{\left(U_i^{\otimes k}\right)^\dagger O_i \, U_i^{\otimes k}} \\
&= \bigotimes_{i=1}^N \Phi^{(k)}_1(O_i) \\
&= \bigotimes_{i=1}^N \sum_{\pi_i, \sigma_i \in S_k} C_{\pi_i,\sigma_i} W_{\pi_i} \mathrm{Tr}\left[W_{\sigma_i} O_i\right]
\end{aligned} \tag{24}$$

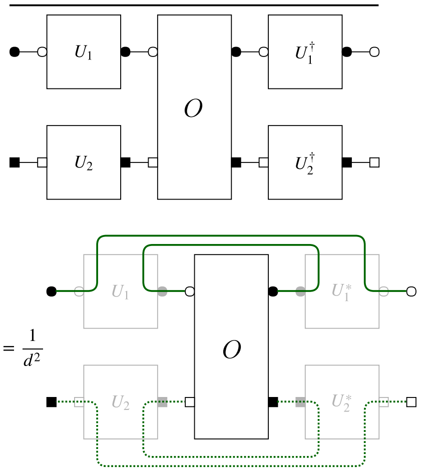

FIG. 7. Graphical evaluation of $\Phi_2^{(1)}$. We evaluate graphically the matrix element $\langle ij|\,\Phi^{(1)}(U)\,|i'j'\rangle$ where only decorations of the same type, corresponding to the same random unitary are connected. For clarity the boxes describing the basis states $\langle ij|$, $|i'j'\rangle$ have been omitted, only their decorations are kept.

and from the last line, Eq. (23) follows.

To treat composite systems with multiple independent random unitaries within the graphical calculus presented in Sec. III B, one introduces decorations of different types (circles, boxes, ...) and connects only decorations of the same type. For an example, we refer to Fig. 7 where $\Phi_2^{(1)}$ is evaluated.

IV. SECOND ORDER CORRELATIONS - PURITY AND OVERLAP OF QUANTUM STATES

In this section, we apply our formalism to derive Eqs. (4) and (5) allowing the estimation of the purity of arbitrary quantum states using the experimental protocol given in Sec. II A. Furthermore, we discuss a extension of the protocol given in Sec. II A, to estimate the overlap of two distinct quantum states. Higher order functionals of the density matrix are discussed in the appendix A.

A. Proof of the main result

We proof now Eqs. (4) and (5). We first note that the case (i) of global random unitaries can be viewed as a single qu$\mathcal{D}$it with dimension $\mathcal{D}_A$. Then, the first line of Eq. (4) follows directly from Eq. (5) by setting $N_A = 1$ and $d \to \mathcal{D}_A = d^{N_A}$, and the second line by using $\sum_{\mathbf{s}',\mathbf{s}'\neq\mathbf{s}} P_U(\mathbf{s}') = 1 - P_U(\mathbf{s})$. Thus, we consider in the following the case (ii) of independent local random unitaries applied to a composite system of N_A qudits with arbitrary local dimension d. For simplicity of notation, we drop the subscript A.

We first note that the ensemble average of second order cross-correlation of outcome probabilities of randomized measurements can be rewritten as an expectation value of an operator O acting on two "virtual copies" and twirled state $\Phi_N^{(2)}(\rho\otimes)$ [with $\Phi_N^{(2)}$ defined in Eq. (23)]. For arbitrary coefficients $O_{\mathbf{s},\mathbf{s}'}$, it holds

$$\begin{aligned}
\sum_{\mathbf{s},\mathbf{s}'} & O_{\mathbf{s},\mathbf{s}'}\ \overline{P_U(\mathbf{s})P_U(\mathbf{s}')} \\
&= \mathrm{Tr}\left[\sum_{\mathbf{s},\mathbf{s}'} O_{\mathbf{s},\mathbf{s}'} \,|\mathbf{s}\rangle\langle\mathbf{s}|\otimes|\mathbf{s}'\rangle\langle\mathbf{s}'|\, \overline{U^{\otimes 2}\rho\otimes\rho\,(U^\dagger)^{\otimes 2}}\right] \\
&= \mathrm{Tr}\left[O\ \Phi_N^{(2)}(\rho\otimes\rho)\right] \\
&= \mathrm{Tr}\left[\Phi_N^{(2)}(O)\ \rho\otimes\rho\right], \qquad (25)
\end{aligned}$$

where we defined the operator $O = \sum_{\mathbf{s},\mathbf{s}'} O_{\mathbf{s},\mathbf{s}'}\,|\mathbf{s}\rangle\langle\mathbf{s}|\otimes|\mathbf{s}'\rangle\langle\mathbf{s}'|$ and used the self-duality of the channel $\Phi_N^{(2)*} = \Phi_N^{(2)}$. Secondly, we observe that, for an arbitrary quantum state ρ, the purity can be rewritten as

$$\mathrm{Tr}\left[\rho^2\right] = \mathrm{Tr}\left[\mathbb{S}\rho\otimes\rho\right], \qquad (26)$$

where $\mathbb{S} = \sum_{\mathbf{s},\mathbf{s}'} |\mathbf{s}'\rangle\langle\mathbf{s}|\otimes|\mathbf{s}\rangle\langle\mathbf{s}'| = W_{(12)^{\otimes N}} = W_{(12)}^{\otimes N}$ is the swap operator acting on two "virtual" copies $\mathcal{H}^{\otimes N}\otimes\mathcal{H}^{\otimes N}$ of the Hilbert space of N qudits. Comparing Eqs. (25) and (26), our goal is thus to find coefficients $O_{\mathbf{s},\mathbf{s}'}$ of the operator O such that

$$\Phi_N^{(2)}(O) = \mathbb{S}. \qquad (27)$$

Since $\Phi_N^{(2)}(o^{\otimes N}) = \left(\Phi_1^{(2)}(o)\right)^{\otimes N}$ factorizes for an operator $O = \otimes_{i=1}^N o$ [Eq. (24)], it is sufficient to find local operators $o = \sum_{s,s'=1}^d o_{s,s'}\,|s\rangle\langle s|\otimes|s'\rangle\langle s'|$ which fulfill

$$\Phi_1^2(o) = W_{(12)}. \qquad (28)$$

Using Eq. (17), this is equivalent to

$$\mathrm{Tr}\left[W_\sigma o\right]=(C_{\sigma,(21)})^{-1} = d^{\sharp\mathrm{cycles}(\sigma,(21))} \quad \forall\sigma\in\mathcal{S}_2\,. \quad (29)$$

Inserting the ansatz $o = \sum_{s,s'=1}^d o_{s,s'}\,|s\rangle\langle s|\otimes|s'\rangle\langle s'|$ into Eq. (29), we find the following equations to be satisfied by the coefficients $o_{s,s'}$

$$\mathrm{Tr}\left[W_{(12)}o\right] = \sum_{s,s'=1}^d o_{s,s'} \overset{!}{=} d$$

and

$$\mathrm{Tr}\left[W_{(21)}o\right] = \sum_{s=1}^d o_{s,s} \overset{!}{=} d^2.$$

These are satisfied by the simple choice

$$o_{s,s'} = (d+1)\delta_{s,s'} - 1 = d(-d)^{-D_G[s,s']},$$

where $D_G[s, s']$ is the Hamming distance of the states s and s' of the single qudit, i.e. $D_G[s, s] = 0$ and $D_G[s, s'] = 1$ if $s \neq s'$. On the composite system, we then simply choose

$$O = o^{\otimes N} = d^N \sum_{\mathbf{s},\mathbf{s}'} (-d)^{-D[\mathbf{s},\mathbf{s}']} \left|\mathbf{s}\right\rangle \left\langle\mathbf{s}\right| \otimes \left|\mathbf{s}'\right\rangle \left\langle\mathbf{s}'\right| , \quad (30)$$

where $D[\mathbf{s}, \mathbf{s}'] = \sum_{i=1}^{N} D_G[s_i, s'_i]$ is the Hamming distance of the states $\mathbf{s}$ and $\mathbf{s}'$ of N qudits. This leads directly to Eq. (5).

B. Scaling of statistical errors

In the previous sections, we have shown how to access the purity of an arbitrary quantum state ρ_A from the ensemble average over cross correlations of outcome probabilities of randomized measurements. Here, we discuss the statistical errors arising in a experiment due to a finite number N_U of unitaries to estimate the ensemble average and a finite number N_M of measurements per random unitary to estimate the probabilities $P_U(\mathbf{s}_A)$.

For the protocol utilizing global random unitaries, we found in Ref. [29] analytically a scaling law of the typical statistical error of the estimated purity of a density matrix ρ_A in a Hilbert space with dimension $\mathcal{D}_A$

$$\left| \left(\mathrm{Tr}\left[\rho_A^2\right]\right)_e - \mathrm{Tr}\left[\rho_A^2\right] \right| \sim \frac{1}{\sqrt{N_U \mathcal{D}_A}} \left(c_1 + c_2 \frac{\mathcal{D}_A}{N_M} \right). \quad (31)$$

where c_1 and c_2 are constants of $\mathcal{O}(1)$ which are largest for pure states. Thus the number of measurements per random unitary required to estimate the purity up to an error of $1/\sqrt{N_U}$ scales as $N_M \sim \sqrt{\mathcal{D}_A}$. The scaling behavior with N_U is hereby a direct consequence of the central limit theorem, whereas the scaling with N_M is directly related to probability of finding doublons when sampling with replacement from a finite probability distribution (the so-called birthday paradox [48]). Note, that we use unbiased estimator to infer the squared outcome probabilities $P_U(\mathbf{s}_A)^2$ from a finite number of measurements N_M [29]. The analytical results are supported by numerical simulations presented in Fig. 8, panels a) and c) where the average statistical error, extracted from 100 numerical experiments, is shown, for a pure and a mixed state. The black lines are calculated from the scaling law (31). Clearly, the statistical error of the mixed state is smaller, which is explained by the fact that fluctuations across the unitary ensemble are reduced for mixed states (with vanishing fluctuations for the maximally mixed state $\rho_{\max} \sim \mathbb{1}/\mathcal{D}_A$).

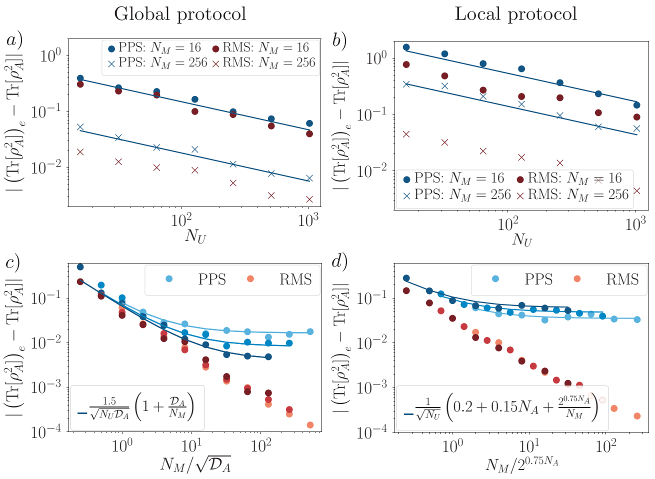

FIG. 8. Statistical errors of the estimated purity of a pure product state (PPS) and a random mixed state (RMS) Panels a) and b) display the statistical errors of the estimated purity using a) global unitaries and b) local unitaries in a system of $N_A = 8$ qubits, as a function of N_U for $N_M = 16$ (dots) and $N_M = 256$ (crosses). Hilbert space dimension is $\mathcal{D} = 2^8$. In panels c) (global unitaries) and d) (local unitaries) the number of unitaries $N_U = 512$ is fixed, and the statistical error is shown as function of the number of measurements N_M. The Hilbert space dimension (number of qubits N_A) increases with darkness of the colors, $\mathcal{D}_A = 2^4, 2^6, 2^8$. Solid lines are calculated from the given scaling laws. Random unitaries are sampled directly from CUE [38]. The RMS of $N_A = 4, 6, 8$ qubits has been obtained by applying a Haar random unitary to a pure product state consisting of 12 qubits, and tracing out the residual $8, 6, 4$ degrees of freedom.

For the protocol utilizing local random unitaries, we find, from numerical simulations, see Fig. 8, panels b) and d), for a pure product state of N_A qubits, a scaling law

$$\left| \left(\mathrm{Tr}\left[\rho_A^2\right]\right)_e - \mathrm{Tr}\left[\rho_A^2\right] \right| \sim \frac{1}{\sqrt{N_U}} \left(c_3 + \frac{2^{0.75 N_A}}{N_M} \right), \quad (32)$$

where $c_3 = \mathcal{O}(N_A)$. The scaling with N_U follows the behavior expected from the central limit theorem. The number of measurements to estimate the purity up to an error $\sim 1/\sqrt{N_U}$ scales as $N_M \sim 2^{0.75 N_A}$, and is thus larger than for the global protocol. However, in contrast to the global protocol, the statistical errors for entangled states of N_A qubits are reduced which is explained by the fact that here the reduced density matrices for subsystems are mixed, and thus fluctuations across the unitary ensemble are locally reduced. Similar as in the global protocol, this holds true if ρ_A itself is mixed.

We note that on the one hand, the local protocol (ii) is more prone to statistical errors compared to the global protocol (i). On the other hand, we can obtain by restriction from the occupation probabilities $P_U(\mathbf{s}_A)$ of basis states $|\mathbf{s}_A\rangle$ of the (sub-)system A, the occupation probabilities $P_U(\mathbf{s}_{A'})$ of basis states $|\mathbf{s}\rangle_{A'}$ of an arbitrary subsystem $A' \subseteq A$. This is not possible for the global protocol, where the applied random unitary U_A randomizing the entire Hilbert space $\mathcal{H}_A$ of ρ_A predefines the (sub-)system of interest.

C. Measurement of the overlap of quantum states

In this subsection, we discuss a natural extension of the protocol presented in Sec. II A to estimate the overlap $\mathrm{Tr}\left[\rho_1\rho_2\right]$ of two distinct quantum states ρ_1 and ρ_2 of N qudits in Hilbertspace $\mathcal{H}$ of dimension $\mathcal{D} = d^N$. To obtain the overlap $\mathrm{Tr}\left[\rho_1\rho_2\right]$, one applies the experimental sequence described in Sec. II A twice with same set of random unitaries, starting first with the state ρ_1 and secondly with the state ρ_2. Repeated for many random unitaries U, this provides the set of occupation probabilities $P_U^{(1)}(\mathbf{s}) = \mathrm{Tr}\left[U\rho_1 U^\dagger \left|\mathbf{s}\right\rangle\left\langle\mathbf{s}\right|\right]$ and $P_U^{(2)}(\mathbf{s}) = \mathrm{Tr}\left[U\rho_2 U^\dagger \left|\mathbf{s}\right\rangle\left\langle\mathbf{s}\right|\right]$ of the computational basis states $\left|\mathbf{s}\right\rangle$. From cross correlations, the overlap is estimated. Generalizing Eqs. (4) and (5), one finds, if (i) global random unitaries have been used

$$\mathrm{Tr}\left[\rho_1\rho_2\right] = \mathcal{D}\sum_{\mathbf{s},\mathbf{s}'}(-\mathcal{D})^{-D_G[\mathbf{s},\mathbf{s}']}\,\overline{P_U^{(1)}(\mathbf{s})P_U^{(2)}(\mathbf{s}')} \tag{33}$$

and (ii) for local random unitaries

$$\mathrm{Tr}\left[\rho_1\rho_2\right] = d^N\sum_{\mathbf{s},\mathbf{s}'}(-d)^{-D[\mathbf{s},\mathbf{s}']}\,\overline{P_U^{(1)}(\mathbf{s})P_U^{(2)}(\mathbf{s}')}. \tag{34}$$

These equation follow directly from the proof presented in Sec. IV A, using that $\mathrm{Tr}\left[\rho_1\rho_2\right] = \mathrm{Tr}\left[\mathbb{S}\rho_1\otimes\rho_2\right]$.

We note that this protocol enables a measurement of the Loschmidt echo $\left|\langle\psi_0|e^{iH_2t/\hbar}e^{-iH_1t/\hbar}|\psi_0\rangle\right|^2$ [30] without the necessity of implementing time reversed operations or ancilla degrees of freedom; the protocol is outlined in the following: In a first experiment, $\left|\psi_0\right\rangle$ is evolved forward in time with Hamiltonian H_1 and after the application of a random unitary U, the probabilities $P_U^{(1)}(\mathbf{s}) = |\left\langle\mathbf{s}|Ue^{-iH_1t/\hbar}|\psi_0\right\rangle|^2$ for the basis states $\left|\mathbf{s}\right\rangle$ are measured. This is then repeated with H_2, and *same* random unitary U, to obtain $P_U^{(2)}(\mathbf{s}) = |\left\langle\mathbf{s}|Ue^{-iH_2t/\hbar}|\psi_0\right\rangle|^2$. The overlap $\left|\langle\psi_0|e^{iH_2t/\hbar}e^{-iH_1t/\hbar}|\psi_0\rangle\right|^2$ is finally inferred from cross-correlations over many random unitaries, according to Eqs. (33) and (34). Thus, there is no the necessity to implement the time reversed evolution operator $e^{iH_2t/\hbar}$ in the experiment.

We further remark that this protocol can be used to check the stability of an experiment is against drifts, by measuring the overlap of two quantum states ρ_1 and ρ_2 which are prepared in the same way, but at different instances of time.

V. RANDOMIZED QUANTUM STATE TOMOGRAPHY

In this section, we describe a protocol to perform full quantum state tomography, based on statistical correlation of randomized measurements. For global random unitaries, this protocol was first described in Ref. [31] in the context of atomic Hubbard models. Here, we focus on spin models and extend the protocol to composite systems of many qudits where local unitaries are applied, and investigate in detail the scaling of the required number of measurements to estimate the density matrix up to a fixed statistical error with the Hilbert space dimension (the number of constituents).

We consider a quantum state ρ_A, which can be a reduced state $\rho_A = \mathrm{Tr}_{\mathcal{S}\backslash A}\left[\rho\right]$ of a subsystem $A\subseteq\mathcal{S}$, defined in the Hilbert space $\mathcal{H}_A = \hbar^{\otimes N_A}$ with total dimension $\mathcal{D}_A = d_A^N$. The use of randomized measurements to perform quantum state tomography is based on the observation that

$$\rho_A = \mathrm{Tr}_2\left[\mathbb{S}\;\mathbb{1}_{\mathcal{H}_A}\otimes\rho_A\right] \tag{35}$$

where S is the swap operator and the partial trace is taken over the second "copy'. Using the results of Sec. IV A, this gives immediately rise to a measurement protocol to perform quantum state tomography using randomized measurements. Employing the ensemble average over *global random* unitaries, randomizing the entire Hilbert space $\mathcal{H}_A$, we find

$$\begin{aligned}\rho_A &= \mathrm{Tr}_2\left[\Phi^{(2)}(O)\;\mathbb{1}_{\mathcal{H}}\otimes\rho\right]\\ &= \mathcal{D}_A\sum_{\mathbf{s}_A,\mathbf{s}'_A}(-\mathcal{D}_A)^{-D_G[\mathbf{s}_A,\mathbf{s}'_A]}\overline{P_U(\mathbf{s}_A)\;U_A\left|\mathbf{s}'_A\right\rangle\left\langle\mathbf{s}'_A\right|U_A^\dagger}\\ &= (\mathcal{D}_A+1)\overline{P_U(\mathbf{s}_A)\;U\left|\mathbf{s}_A\right\rangle\left\langle\mathbf{s}_A\right|U_A^\dagger} - \frac{\mathbb{1}_{\mathcal{H}_A}}{\mathcal{D}_A}.\end{aligned} \tag{36}$$

where the expression in the last line was first obtained in Ref. [31]. If we consider instead local random unitaries $U = \bigotimes_{i=1}^{N_A}U_i$ where the U_i are sampled independently from CUE($\hbar$), we find

$$\begin{aligned}\rho_A &= \mathrm{Tr}_2\left[\Phi_{N_A}^{(2)}(O)\,\mathbb{1}_{d^{N_A}}\otimes\rho\right]\\ &= d^{N_A}\sum_{\mathbf{s}_A,\mathbf{s}'_A}(-d)^{-D[\mathbf{s}_A,\mathbf{s}'_A]}\overline{P_U(\mathbf{s}_A)\;U_A\left|\mathbf{s}'_A\right\rangle\left\langle\mathbf{s}'_A\right|U_A^\dagger}.\end{aligned} \tag{37}$$

The experimental protocol reads thus as follows. Given the quantum state ρ_A a random unitary U_A, being either local or global, is applied. Subsequently, a measurement in the computational basis is performed. This is repeated with the same random unitary, to access the occupation probabilities $P_U(\mathbf{s}_A)$ of the computational basis states $\left|s\right\rangle_A$. Additionally, the random unitary U_A is stored as a matrix in the computational basis. Finally, the ensemble average is performed, as in Eqs. (36) and (37).

We emphasize that, in contrast to the previously discussed protocols, the tomographic reconstruction of ρ_A from randomized measurements requires the explicit knowledge of the applied unitaries in a specific basis, i.e. not only their property of being sampled from an appropriate random matrix ensemble. The tomographic reconstruction is thus prone to experimental imperfections

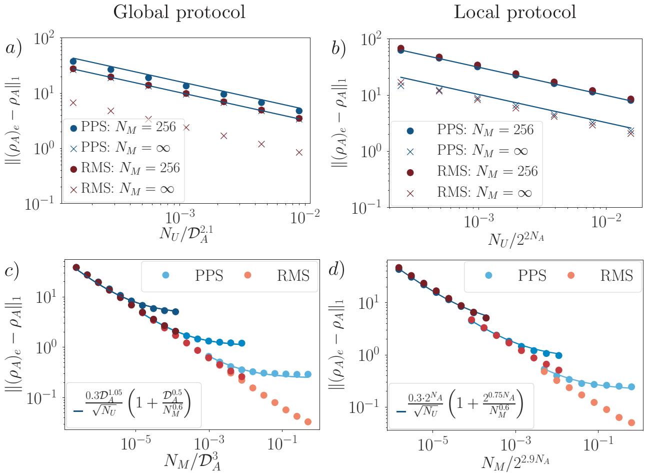

FIG. 9. Statistical errors of the reconstructed density matrix for a pure product state (PPS) and a random mixed state (RMS). Panels a) and b) present the average deviation of the reconstructed density matrix using a) global unitaries and b) local unitaries in a system of $N_A = 8$ qubits ($\mathcal{D}_A = 2^8$), as a function of N_U for $N_M = 16$ (dots) and $N_M = 256$ (crosses). In panels c) (global unitaries) and d) (local unitaries) the number of unitaries $N_U = 512$ is fixed, and the average statistical error is shown as function of the number of measurements N_M. The Hilbert space dimension (number of qubits N_A) increases with darkness of the colors, $\mathcal{D}_A = 2^4, 2^6, 2^8$. Solid lines are calculated from the given scaling laws. Random unitaries are sampled directly from CUE [38]. The RMS of $N_A = 4, 6, 8$ qubits has been obtained by applying a Haar random unitary to a pure product state consisting of 12 qubits, and tracing out the residual $8, 6, 4$ degrees of freedom.

which lead to a (random) mismatch between the “applied” random unitary and the one “stored” to reconstruct ρ_A. In general, such decorrelation will appear as depolarizing noise, i.e. induces a bias towards mixed state. This is not the case for protocols which detect properties of ρ_A which are invariant under unitary transformations, such as the purity estimation.

A crucial aspect for any measurement scheme providing tomographic reconstruction of a quantum state is the scaling of the required number of measurements with system size. In the protocol presented here, the accuracy of an estimation $(\rho_A)_e$, quantified by the trace distance $\|(\rho_A)_e - \rho\|_1$ to the true state ρ_A, is determined by statistical errors originating from a finite number of random unitaries N_U and a finite number of measurements N_M per random unitary. In Fig. 9, the scaling behavior of the trace distance of the estimated density matrix $(\rho_A)_e$ for a pure product state ρ_A is shown. For both protocols, we find that the numerical data, obtained with random unitaries sampled directly from the CUE [38], is well described by a scaling law

$$\|(\rho_A)_e - \rho_A\|_1 \sim \frac{\mathcal{D}_A^a}{\sqrt{N_U}}\left(1 + \frac{\mathcal{D}_A^b}{N_M^{0.6}}\right), \qquad (38)$$

where for the global protocol, $a \approx 1.05$, $b \approx 0.5$, and for the local protocol $a \approx 1.0$, $b \approx 0.75$. From Eq. (38) it follows directly that, for pure product states, the required number of random unitaries N_U scales as $\mathcal{D}_A^2 = 2^{2N_A}$ and is thus comparable to the mininmal number of measurement settings in standard tomography [8]. As shown in Fig. 9, the statistical errors of an estimation of ρ_A depend in general on the quantum state, where (absolute) errors smaller for mixed states (see also [16, 29]). We note that it was shown in Ref. [31] that the above protocols for randomized state tomography can be combined with compressed sensing [8] to decrease the number of required measurements.

VI. CONCLUSION

We have introduced statistical correlations of randomized measurements as a new tool to probe complex many-body quantum states. While we have focused on measurements protocol accessing bipartite entanglement of quantum states and their tomographics reconstructions, the underlying tools can be applied more generally. In a recent paper [49], we use statistical correlations to design robust protocols to measure out-of-time ordered correlation functions, without the necessity to implement time-reversed operations or ancilla degrees of freedom. In the future, the paradigm of statistical correlation could be extended to the measurement of order parameters in (symmetry protected) topological phases [50–53] and the estimation of the entanglement spectrum [54–56].

Our protocols can be applied in state-of-the-art quantum simulators with single site read-out and control. As they rely on statistical correlations of many random measurements, they are particularly suitable for systems with high repetition rates such as trapped-ions, superconducting qubits and Rydberg atoms. In atomic Hubbard models, one can take advantage of the possibility to prepare simultaneously many (independent) copies of the quantum systems to reduce the number of experimental runs.

Furthermore, it would be interesting to extend the protocol based on local unitaries to models with (locally) conserved quantum numbers. For instance, local random unitaries with conserved particle number could be generated in atomic Hubbard models, by isolating pairs of sites and applying to each a series of random quenches.

ACKNOWLEDGMENTS

We thank B. Kraus, L. Sieberer and J. Yu for discussions. Our work is supported by the ERC Synergy Grant UQUAM, the SFB FoQuS (FWF Project No. F4016-N23), QTFLAG - QuantERA and the Quantum Flagship project PASQuanS. C.F. Roos acknowledges funding from the European Research Council (ERC grant agreement No. 741 541) and the EU Horizon 2020 program. Numerical simulations were realized with QuTiP [57].

[1] J. Preskill, Quantum **2**, 79 (2018).

[2] I. Bloch, J. Dalibard, and S. Nascimbène, Nat. Phys. **8**, 267 (2012).

[3] R. Blatt and C. F. Roos, Nature Physics **8**, 277 (2012).

[4] A. Browaeys, D. Barredo, and T. Lahaye, Journal of Physics B: Atomic, Molecular and Optical Physics **49**, 152001 (2016).

[5] J. M. Gambetta, J. M. Chow, and M. Steffen, npj Quantum Information **3**, 2 (2017).

[6] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Rev. Mod. Phys. **81**, 865 (2009).

[7] H. Häffner, W. Hänsel, C. F. Roos, J. Benhelm, D. Chek-Al-Kar, M. Chwalla, T. Körber, U. D. Rapol, M. Riebe, P. O. Schmidt, C. Becher, O. Gühne, W. Dür, and R. Blatt, Nature (London) **438**, 643 (2005).

[8] D. Gross, Y.-K. Liu, S. T. Flammia, S. Becker, and J. Eisert, Phys. Rev. Lett. **105**, 150401 (2010).

[9] B. P. Lanyon, C. Maier, M. Holzäpfel, T. Baumgratz, C. Hempel, P. Jurcevic, I. Dhand, A. S. Buyskikh, A. J. Daley, M. Cramer, M. C. Plenio, R. Blatt, and C. F. Roos, Nat. Phys. **13**, 1158 (2017).

[10] G. Torlai, G. Mazzola, J. Carrasquilla, M. Troyer, R. Melko, and G. Carleo, Nat. Phys. **14**, 447 (2018).

[11] R. Islam, R. Ma, P. M. Preiss, M. E. Tai, A. Lukin, M. Rispoli, and M. Greiner, Nature **528**, 77 (2015).

[12] A. M. Kaufman, M. E. Tai, A. Lukin, M. Rispoli, R. Schittko, P. M. Preiss, and M. Greiner, Science **353**, 794 (2016).

[13] F. A. Bovino, G. Castagnoli, A. Ekert, P. Horodecki, C. M. Alves, and A. V. Sergienko, Phys. Rev. Lett. **95**, 240407 (2005).

[14] A. J. Daley, H. Pichler, J. Schachenmayer, and P. Zoller, Phys. Rev. Lett. **109** (2012).

[15] H. Pichler, L. Bonnes, A. J. Daley, A. M. Läuchli, and P. Zoller, New Journal of Physics **15**, 063003 (2013).

[16] T. Brydges, A. Elben, P. Jurcevic, B. Vermersch, C. Maier, B. P. Lanyon, P. Zoller, R. Blatt, and C. F. Roos, arXiv:1806.05747.

[17] A. Elben, B. Vermersch, M. Dalmonte, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **120**, 050406 (2018).

[18] J. Zhang, G. Pagano, P. W. Hess, A. Kyprianidis, P. Becker, H. Kaplan, A. V. Gorshkov, Z.-X. Gong, and C. Monroe, Nature **551**, 601 (2017).

[19] J. Zeiher, J.-y. Choi, A. Rubio-Abadal, T. Pohl, R. van Bijnen, I. Bloch, and C. Gross, Physical Review X **7**, 041063 (2017).

[20] D. Barredo, V. Lienhard, S. De Leseleuc, T. Lahaye, and A. Browaeys, Nature **561**, 79 (2018).

[21] E. Guardado-Sanchez, P. T. Brown, D. Mitra, T. Devakul, D. A. Huse, P. Schauß, and W. S. Bakr, Physical Review X **8**, 021069 (2018).

[22] A. Keesling, A. Omran, H. Levine, H. Bernien, H. Pichler, S. Choi, R. Samajdar, S. Schwartz, P. Silvi, S. Sachdev, *et al.*, arXiv:1809.05540 .

[23] J. Z. Blumoff, K. Chou, C. Shen, M. Reagor, C. Axline, R. T. Brierley, M. P. Silveri, C. Wang, B. Vlastakis, S. E. Nigg, L. Frunzio, M. H. Devoret, L. Jiang, S. M. Girvin, and R. J. Schoelkopf, Phys. Rev. X **6**, 031041 (2016).

[24] R. Barends, A. Shabani, L. Lamata, J. Kelly, A. Mezzacapo, U. Las Heras, R. Babbush, A. G. Fowler, B. Campbell, Y. Chen, *et al.*, Nature **534**, 222 (2016).

[25] J. Otterbach, R. Manenti, N. Alidoust, A. Bestwick, M. Block, B. Bloom, S. Caldwell, N. Didier, E. S. Fried, S. Hong, *et al.*, arXiv:1712.05771 .

[26] M. Gong, M.-C. Chen, Y. Zheng, S. Wang, C. Zha, H. Deng, Z. Yan, H. Rong, Y. Wu, S. Li, *et al.*, arXiv preprint arXiv:1811.02292 (2018).

[27] S. J. van Enk and C. W. J. Beenakker, Phys. Rev. Lett. **108**, 110503 (2012).

[28] Y. Nakata, C. Hirche, M. Koashi, and A. Winter, Phys. Rev. X **7**, 021006 (2017).

[29] B. Vermersch, A. Elben, M. Dalmonte, J. I. Cirac, and P. Zoller, Phys. Rev. A **97**, 023604 (2018).

[30] A. Goussev, R. A. Jalabert, H. M. Pastawski, and D. Wisniacki, arXiv:1206.6348.

[31] M. Ohliger, V. Nesme, and J. Eisert, New J. Phys. **15** (2013).

[32] We note that this criterium is sufficient but not necessary.

[33] P. Horodecki, Phys. Rev. A **68**, 052101 (2003).

[34] N. M. Linke, S. Johri, C. Figgatt, K. A. Landsman, A. Y. Matsuura, and C. Monroe, Phys. Rev. A **98**, 052334 (2018).

[35] D. Gross, K. Audenaert, and J. Eisert, J. Math. Phys. **48** (2007).

[36] C. Dankert, R. Cleve, J. Emerson, and E. Livine, Phys. Rev. A **80**, 012304 (2009).

[37] O. Gamel, Phys. Rev. A **93**, 062320 (2016).

[38] F. Mezzadri, Notices of the AMS **54**, 592 (2007).

[39] D. A. Roberts and B. Yoshida, J. High Energy Phys. **2017** (2017).

[40] Intuitively, Haar random unitaries are matrices with elements whose real and imaginary parts are independently distributed according to a normal distribution, with additional unitary constraints on the entire matrix.

[41] F. Haake, *Quantum Signatures of Chaos*, Springer Series in Synergetics (Springer Berlin Heidelberg, 2010).

[42] B. Collins and I. Nechita, Commun. Math. Phys. **297**, 345 (2010).

[43] Z. Puchała and J. A. Miszczak, Bull. Polish Acad. Sci. Tech. Sci. **65**, 21 (2017).

[44] P. W. Brouwer and C. W. Beenakker, J. Math. Phys. **37**, 4904 (1996).

[45] Note that for clarity, we omitted here the boxes of basis states, and just kept the decorations.

[46] A. Roy and A. J. Scott, Des. Codes, Cryptogr. **53**, 13 (2009).

[47] Loosely speaking, up to the kth moment, k-designs are as random as Haar random unitaries.

[48] S. M. Blinder, *Guide to Essential Math: A Review for Physics, Chemistry and Engineering Students* (Elsevier, 2013).

[49] B. Vermersch, A. Elben, L. M. Sieberer, N. Y. Yao, and P. Zoller, arXiv:1807.09087.

[50] X. Chen, Z.-C. Gu, Z.-X. Liu, and X.-G. Wen, Science **338**, 1604 (2012).

[51] F. Pollmann and A. M. Turner, Phys. Rev. B **86**, 125441 (2012).

[52] J. Haegeman, D. Pérez-García, I. Cirac, and N. Schuch, Phys. Rev. Lett. **109**, 050402 (2012).

[53] H. Shapourian, K. Shiozaki, and S. Ryu, Phys. Rev. Lett. **118**, 216402 (2017).

[54] H. Li and F. D. M. Haldane, Phys. Rev. Lett. **101**, 010504

(2008).

[55] H. Pichler, G. Zhu, A. Seif, P. Zoller, and M. Hafezi, Phys. Rev. X **6**, 041033 (2016).

[56] M. Dalmonte, B. Vermersch, and P. Zoller, Nature Physics , 1 (2018).

[57] J. R. Johansson, P. D. Nation, and F. Nori, Comput. Phys. Commun. **184**, 1234 (2013).

[58] M. Bona, *Combinatorics of Permutations, Second Edition*, Discrete Mathematics and Its Applications (CRC Press, 2016).

Appendix A: Higher order Rényi entropies

In this section, we discuss the estimation of kth-order functionals $\mathrm{Tr}\left[\rho^k\right]$ ($k \in \mathbb{N}, k \geq 2$) from statistical correlations of globally randomized measurements, which are directly connected to k-th order Rényi entropies $S^{(k)}(\rho) = 1/(1-k)\log_2 \mathrm{Tr}\left[\rho^k\right]$.

The experimental sequence is the same as described in section II A. Global random unitaries U sampled from a *unitary k-design* defined on the entire Hilbert space $\mathcal{H}$ are applied to the quantum state ρ and subsequently occupation probabilities $P_U(\mathbf{s})$ are measured. In Ref. [29] we showed that the k-th moment $\overline{P_U(s)^k}$ is related to $\mathrm{Tr}\left[\rho^k\right]$

$$\overline{P_U(s)^k} = \frac{1}{\mathcal{D}_k} \sum C_{b_1,\dots,b_k} \prod_{l=1}^{k} \mathrm{Tr}\left[\rho^l\right]^{b_l} \qquad \text{(A1)}$$

where $\mathcal{D}_k = \prod_{i=0}^{k-1}(\mathcal{D}+i)$ and $C_{b_1,\dots,b_k}$ denotes the number of permutations $\sigma \in S_k$ with $\mathrm{typ}(\sigma) = 1^{b_1}2^{b_2}\dots k^{b_k}$ and is given by [58]

$$C_{b_1,\dots,b_k} = \frac{k!}{b_1!\cdot b_2!\cdot \ldots \cdot b_k! \cdot 1^{b_1}\cdot 2^{b_2}\cdot \ldots \cdot k^{b_k}}\ . \qquad \text{(A2)}$$

This result is easily recovered with the help of the results of section III. We obtain

$$\begin{aligned}
\overline{P_U(s)^k} &= \mathrm{Tr}\left[\Phi_1^{(k)}\left(\rho^{\otimes k}\right)|s\rangle\langle s|^{\otimes k}\right] \\
&= \mathrm{Tr}\left[\Phi_1^{(k)}\left(|s\rangle\langle s|^{\otimes k}\right)\rho^{\otimes k}\right] \\
&= \frac{1}{\mathcal{D}_k}\sum_{\sigma\in S_k}\mathrm{Tr}\left[W_\sigma \rho^{\otimes k}\right] \qquad \text{(A3)}\\
&= \frac{1}{\mathcal{D}_k}\sum C_{b_1,\dots,b_k}\prod_{l=1}^{k}\mathrm{Tr}\left[\rho^l\right]^{b_l} \qquad \text{(A4)}
\end{aligned}$$

where we used that $\sum_{\pi\in S_k} C_{\pi\sigma} = 1/\prod_{i=0}^{k-1}(\mathcal{D}+i) \equiv 1/\mathcal{D}_k$ and $\mathrm{Tr}\left[W_\sigma |s\rangle\langle s|^{\otimes k}\right] = 1$ for any $\sigma \in S_k$. Since any unitary k-design is also a unitary l-design for $l < k$, we can reconstruct $\mathrm{Tr}\left[\rho_A^l\right]$ for $l < k$ from lower order moments $P_U(s)^l$. Thus, Eq. (A4) can be solved recursively to obtain $\mathrm{Tr}\left[\rho^k\right]$.

In contrast to the case of global unitaries, the generalization of our method to access $\mathrm{Tr}\left[\rho^k\right]$ with local unitaries is not straightforward, and will be studied in future work.