Quantifying multiparticle entanglement with randomized measurements

Sophia Ohnemus [1], Heinz-Peter Breuer [1,2] and Andreas Ketterer [1,2,3,*]

[1]*Physikalisches Institut, Albert-Ludwigs-Universität Freiburg, Hermann-Herder-Straße 3, 79104 Freiburg, Germany*
[2]*EUCOR Centre for Quantum Science and Quantum Computing, Albert-Ludwigs-Universität Freiburg,*
Hermann-Herder-Straße 3, 79104 Freiburg, Germany
[3]*Fraunhofer Institute for Applied Solid State Physics IAF, Tullastraße 72, 79108 Freiburg, Germany*

Randomized measurements constitute a simple measurement primitive that exploits the information encoded in the outcome statistics of samples of local quantum measurements defined through randomly selected bases. In this work we exploit the potential of randomized measurements in order to probe the amount of entanglement contained in multiparticle quantum systems as quantified by the multiparticle concurrence. We further present a detailed statistical analysis of the underlying measurement resources required for a confident estimation of the introduced quantifiers using analytical tools from the theory of random matrices. The introduced framework is demonstrated by a series of numerical experiments analyzing the concurrence of typical multiparticle entangled states as well as of ensembles of output states produced by random quantum circuits. Finally, we examine the multiparticle entanglement of mixed states produced by noisy quantum circuits consisting of single- and two-qubit gates with nonvanishing depolarization errors, thus showing that our framework is directly applicable in the noisy intermediate-scale regime.

I. INTRODUCTION

The multiparticle entanglement content of composite quantum states of many, possibly interacting particles plays a central role in the development of novel quantum technologies, ranging from quantum communication protocols to quantum computing architectures [1–4]. For instance, multiparticle entanglement has been shown to enhance the performance of anonymous conference key agreement [5] and act as a resource in quantum metrology [6], and it is believed to be a crucial ingredient in quantum computation algorithms outperforming analogous classical counterparts [7]. However, determining a state's content of multiparticle entanglement becomes increasingly difficult with growing particle number due to the large dimension and immense complexity of the underlying multiparticle Hilbert space [8,9].

Methods for the characterization of multiparticle properties vary strongly in terms of the required measurement resources as well as their assumptions about the states under consideration [10]. While tomographic tools assume very little about the considered quantum states, they become impractical for rather small system sizes [11]. In contrast, witness operators allow for an efficient certification of multiparticle properties, such as structures of entanglement or the states' fidelities, but their successful implementation relies heavily on the knowledge of the investigated quantum states [9,12,13]. Other compromises between these two extreme strategies allow us to lower the required measurement resources by either invoking specific prior information about the sparsity of the involved

density operators [14,15] or accepting limited precision requirements of the targeted observables [16].

A promising approach in this regard is based on so-called randomized measurements where the underlying quantum state is read out in randomly selected local measurement bases and system properties are inferred via appropriate statistical averages [17–42] (see Fig. 1). In this way it has been shown to be possible to extract a number of relevant properties of the underlying many-body states such as structures of multiparticle entanglement [25,26,37,38], subsystem purities [30,31], fidelities with respect to given target states or other quantum devices [18,34], or interference signatures of indistinguishable particles [23,24]. Furthermore, the underlying measurement resources for a statistically significant verification of the aforementioned properties have been investigated, promising advantages particularly in the noisy intermediate-scale regime [35,38,43–45].

In this work we use locally randomized measurements in order to directly extract information about the amount of entanglement in terms of the multiparticle concurrence [46–51], a quantifier for multiparticle entanglement. In particular, we derive an exact formula for the multiparticle concurrence of pure states, as well as for an appropriate lower bound in the case of mixed states, from second moments of the outcomes of random measurements. Furthermore, we analyze in detail the measurement resources required for a statistically confident estimation of the involved quantities by analyzing the respective variances. We apply the developed toolbox to evaluate the multiparticle entanglement of typical multiparticle states and ensembles of states produced by different classes of random quantum circuits (see Fig. 1). Finally, we investigate the multiparticle entanglement of mixed
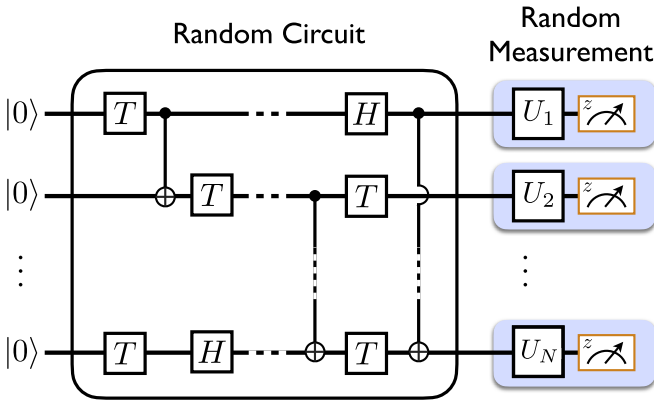
*andreas.ketterer@iaf.fraunhofer.de

FIG. 1. Random quantum circuit consisting of N qubits. The qubits are initialized in the ground state $|0\rangle^{\otimes N}$ and subsequently manipulated with gates drawn from the universal gate set $\mathcal{I}_{\text{uni}} = \{H, T, C_X\}$ which are applied to randomly selected qubits. The resulting output state of the computation is analyzed using a randomized measurement protocol consisting of randomly drawn local unitary transformations U_i complemented with a measurement in the computational basis of N qubits.

states produced by noisy quantum circuits consisting of gates prone to nonvanishing depolarization errors.

The paper is structured as follows. In Sec. II we introduce the paradigm of randomized measurements and show how it enables a measurement of the concurrence of pure multiparticle quantum states and of a suitable lower bound in the case of mixed states. In Sec. III we discuss the statistical estimation of the involved quantities based on finite samples of randomized measurements and in particular analyze the involved statistical error through evaluation of the variances of the respective estimators. In Secs. IV and V we demonstrate the introduced protocols through numerical simulations of typical examples of multiparticle entangled states and ensembles of states produced by random quantum circuits, respectively. We summarize our work in Sec. VI and give a brief outlook for future work.

II. PROBING MULTIPARTICLE ENTANGLEMENT WITH RANDOMIZED MEASUREMENTS

A. Randomized measurements and moments of random correlations

To start with we introduce briefly the framework of randomized measurements as a diagnostic tool for the characterization of multiparticle quantum systems. For reasons of generality we consider in this section a collection of N d-dimensional quantum systems (qudits), each described by a local Hilbert space $\mathcal{H} = \mathbb{C}^d$. The quantum state of the total multiparticle particle system is then described by a density operator ϱ acting on the N-particle Hilbert space $\mathcal{H}^{\otimes N}$.

A random measurement of the N-particle state ϱ is then described through a set of randomly drawn local bases $\{\mathcal{B}_n\}_{n=1,\dots,N}$, each defined as $\mathcal{B}_n = \{U_n|s_n\rangle\}_{s=0,\dots,d-1}$ with a random transformation U_n picked uniformly from the unitary group $\mathrm{U}(d)$, i.e., according to the Haar measure, where $\{|s_n\rangle\}_{s=0,\dots,d-1}$ denotes the computational basis of the nth

qudit. The outcome of a single measurement run in such a random basis is then labeled by a string $\boldsymbol{s} = (s_1, \dots, s_N)$ of length N containing values $s_k = 0, \dots, d-1$ and the associated outcome probability reads $P_U(\boldsymbol{s}) = \mathrm{tr}(\varrho U|\boldsymbol{s}\rangle\langle\boldsymbol{s}|U^\dagger)$, with $U = U_1 \otimes \cdots \otimes U_N$.

The idea behind randomized measurement protocols is now to regard appropriate combinations of the population probabilities $P_U(\boldsymbol{s}) = \mathrm{tr}(\varrho U|\boldsymbol{s}\rangle\langle\boldsymbol{s}|U^\dagger)$ in such a way that, upon averaging them uniformly over the local unitary group $\mathrm{U}(d)^{\otimes N}$, they provide insights about the properties of the quantum state ϱ. For instance, it has been shown in Refs. [30,31] that the state's purity can be obtained as

$$\mathrm{tr}(\varrho^2) = d^N \sum_{\boldsymbol{s},\boldsymbol{s}'} (-d)^{-D(\boldsymbol{s},\boldsymbol{s}')} \mathbb{E}_U[P_U(\boldsymbol{s})P_U(\boldsymbol{s}')], \quad (1)$$

where $D(\boldsymbol{s}, \boldsymbol{s}') = \#\{i \in \{1, \dots, N\} | s_i \neq s_j\}$ denotes the Hamming distance between two computational basis states $|\boldsymbol{s}\rangle = |s_1, \dots, s_N\rangle$ and $|\boldsymbol{s}'\rangle = |s'_1, \dots, s'_N\rangle$ and

$$\mathbb{E}_U[\cdots] = \int_{\mathrm{U}(d)} d\eta(U_1) \cdots \int_{\mathrm{U}(d)} d\eta(U_k) \cdots \quad (2)$$

denotes the average with respect the local Haar measures η over the local unitary group $\mathrm{U}(d)^{\otimes N}$.

Analogously, we can associate a random measurement of a single qudit with an observable $\mathcal{O}_U = U\mathcal{O}U^\dagger$, where $U \in \mathrm{U}(d)$ and $\mathcal{O}$ denotes a traceless observable diagonal in the computational basis with outcomes $\{o_i\}_{i=0,\dots,d-1}$. For instance, for qubits ($d = 2$) a standard choice of the observable $\mathcal{O}$ is given by the Pauli matrix σ_z, leading to the random Pauli matrix $\sigma_{\boldsymbol{u}_i}$, with $[\boldsymbol{u}_i]_j = \mathrm{tr}(\sigma_j U_i \sigma_z U_i^\dagger)$. One round of such a random measurement of N qudits thus allows one obtain the correlation functions

$$\langle \mathcal{O}_{U_{i_1}}^{(i_1)} \cdots \mathcal{O}_{U_{i_k}}^{(i_k)} \rangle = \sum_{\boldsymbol{s}} o_{s_{i_1}} \cdots o_{s_{i_k}} P_U(\boldsymbol{s}), \quad (3)$$

with a subset $A = \{i_1, \dots, i_k\} \subset \{1, \dots, N\}$ of the N qudits of cardinality k. Note that Eq. (3) amounts to a classical postprocessing of the outcome probabilities $P_U(\boldsymbol{s})$, which simplifies significantly in the case of binary observables ($o_s = \pm 1$), where one has to consider overall only two cases, namely, those where the parity of the outcomes is either even or odd [38]. Repeating the above measurement strategy many times for randomly selected choices of U_i then results in a distribution of values which encodes the correlations properties of the state ϱ and is characterized by the moments

$$\mathcal{R}_A^{(t)} = \int_{\mathrm{U}(d)} d\eta(U_1) \cdots \int_{\mathrm{U}(d)} d\eta(U_k) \langle \mathcal{O}_{U_1}^{(i_1)} \cdots \mathcal{O}_{U_k}^{(i_k)} \rangle^t, \quad (4)$$

where t is a positive integer.

The moments (4) have been previously shown to be good candidates for the characterization of multiparticle correlations [21,25,26,37,38]. In particular, it was shown that the combination of moments of different order leads to an improved sensitivity in the sense that a larger class of states can be detected [25,26,37]. Furthermore, it is often useful to combine moments evaluated on different subsets A of qudits in order to obtain more information about the underlying state (see Refs. [31,33,37,42,52]). For instance, the purity formula (1) can be expressed as a sum over second-order reduced

moments of all subsets of qudits, yielding

$$\text{tr}(\varrho^2) = \frac{1}{d^N} \sum_{A \subset \{1,\ldots,N\}} (d^2-1)^{|A|} \mathcal{R}_A^{(2)}(\varrho), \qquad (5)$$

where $\mathcal{R}_\emptyset^{(2)} \equiv 1$, with $\emptyset$ denoting the empty set. In this spirit we will proceed in the following and show that the multiparticle entanglement content, as quantified by multiparticle concurrence, can be assessed via such a randomized measurement protocol.

B. Multiparticle concurrence from randomized measurements

The multiparticle concurrence of an N-qudit pure state $|\psi\rangle \in \mathcal{H}^{\otimes N}$ was introduced in Refs. [46–48] and can be expressed as

$$C_N(|\psi\rangle) = 2 \sqrt{1 - \frac{1}{2^N} \sum_{A \subseteq \{1,\ldots,N\}} \text{tr}(\varrho_A^2)}, \qquad (6)$$

where $\varrho_A = \text{tr}_{A^c}(|\psi\rangle\langle\psi|)$, with $A^c = \{1,\ldots,N\} \setminus A$, denotes the reduced density matrix of the pure state $|\psi\rangle$ with respect to the subsystem associated with the subset A of the N qudits. In Appendix A 1 we show that $C_N(|\psi\rangle)$ can be inferred through the quantity

$$C_N(|\psi\rangle) = 2 \sqrt{1 - \frac{d^N(d+1)^N}{2^N} \mathbb{E}_U\left[P_U^2(\mathbf{s})\right]}, \qquad (7)$$

where $\mathbb{E}_U[\cdots]$ denotes the average over the ensemble of local unitary transformations $U = U_1 \otimes \cdots \otimes U_N$, with $U_i \in \text{U}(d)$, with respect to the local Haar measures on $\text{U}(d)$. Hence, we have found an expression of the multiparticle concurrence (6) that involves only quantities accessible via randomized measurements and thus avoids the evaluation of the purities of all possible partitions of the N involved subsystems. We note that the expression (7) was noted previously in Refs. [53,54]. Alternatively, we can express the concurrence in terms of the moments (4) (see Appendix A 1 for more details), yielding

$$C_N(|\psi\rangle) = 2 \sqrt{1 - \sum_{A \subset \{1,\ldots,N\}} \sum_{A' \subset A} \frac{(d^2-1)^{|A'|}}{2^N d^{|A|}} \mathcal{R}_{A'}^{(2)}}. \qquad (8)$$

Further, generalizations of Eq. (7) to the case of mixed states usually involve a convex roof construction of the form $C(\varrho) = \inf_{\{p_k,|\phi_k\rangle\}} \sum_k p_k C(|\phi_k\rangle)$, where the infimum has to be taken over all possible decompositions $\varrho = \sum_k p_k |\phi_k\rangle\langle\phi_k|$, which is hard to evaluate in practice. This problem can be partially circumvented by considering an appropriate lower bound of the mixed state concurrence $C_N(\varrho)$ as has been derived in Refs. [49–51], leading to the expression

$$C_N(\varrho) \geqslant \sqrt{\text{tr}(\varrho \otimes \varrho V_N)}, \qquad (9)$$

with

$$V_N = 4[\mathbf{P}_+ - P_+ \otimes \cdots \otimes P_+ - (1 - 2^{1-N})\mathbf{P}_-], \qquad (10)$$

where $\mathbf{P}_+$ ($\mathbf{P}_-$) denotes the projector onto the (anti)symmetric subspace of the twofold tensor copy space $(\mathbb{C}^d)^{\otimes N} \otimes (\mathbb{C}^d)^{\otimes N}$ and similarly P_+ (P_-) of the individual qudit subspaces. We note that the bound (9) performs best in the weakly mixed

regime [55] and it is directly accessible via randomized measurements. In Appendix A 1 we thus show that the lower bound (9) can be expressed as

$$C_N(\varrho)^2 \geqslant \frac{4}{2^N} - 2^{2-N} d^N (d+1)^N \mathbb{E}_U\left[P_U^2(\mathbf{s})\right]$$
$$+ \left(4 - \frac{4}{2^N}\right) d^N \sum_{\mathbf{s},\mathbf{s}'} (-d)^{-D(\mathbf{s},\mathbf{s}')} \mathbb{E}_U[P_U(\mathbf{s})P_U(\mathbf{s}')], \qquad (11)$$

with the Hamming distance $D(\mathbf{s},\mathbf{s}')$. Note that the last term in Eq. (11) can be identified as the purity of ϱ [see Eq. (1)] according to the randomized measurement framework introduced in Refs. [28–30]. Again, we can express Eq. (11) equivalently in terms of the moments (4) by combining Eqs. (1) and (8), leading to

$$C_N(\varrho)^2 \geqslant 2(1 - 2^{1-N})$$
$$\times \sum_{A \subset \{1,\ldots,N\}} \left\{ \sum_{A' \subset A} \frac{3^{|A'|}}{2^{|A|}} \mathcal{R}_{A'}^{(2)} + \frac{2 \times 3^{|A|}}{2^N} \mathcal{R}_A^{(2)} \right\}. \qquad (12)$$

Note that an evaluation of the concurrence or its lower bound through finite samples of randomized measurements using Eq. (7) or (11), or equivalently using Eq. (8) or (12), requires the definition of appropriate unbiased estimators which come with a nonvanishing statistical error (see Sec. III).

C. Exact evaluation with quantum designs

The above-introduced formulas for the evaluation of the multiparticle concurrence based on randomized measurement also provide the starting point for the derivation of exact expressions, allowing us to determine the concurrence based on a finite number of measurement settings. To do so, we exploit the concept of unitary designs which provide finite sets of unitary matrices that are inequivalent to Haar random ones as long as one is concerned with statistical moments of some finite order.

Formally, a unitary t-design is a set of unitary matrices $\{U_k | k = 1,\ldots,K^{(t)}\} \subset \text{U}(d)$, with cardinality $K^{(t)}$ [56] such that

$$\frac{1}{K^{(t)}} \sum_{k=1}^{K^{(t)}} P_{t',t'}(U_k) = \int_{\text{U}(d)} P_{t',t'}(U) d\eta(U), \qquad (13)$$

for all homogeneous polynomials $P_{t',t'} \in \mathcal{H}(t',t')$, with $t' \leqslant t$, and where $\eta(U)$ denotes the normalized Haar measure on $\text{U}(d)$. We note that $P_{r,s}(U)$ is an element of the set of all homogeneous polynomials $\mathcal{H}(r,s)$, with support on the space of unitary matrices $\text{U}(d)$, which is of degree at most r and s in each of the matrix elements of U and their complex conjugates, respectively. While the existence of unitary designs has been proven [57], no universal strategy for their construction in the case of an arbitrarily given t is known. However, a number of approximate unitary designs, for which the property (13) is accordingly relaxed, have been introduced in the literature [58–60]. In the remainder of this paper we will restrict ourselves to the particular case of the Clifford group $\mathcal{C}(d) \subset \text{U}(d)$, which has been shown to constitute a unitary

3-design [61,62]. The Clifford group consists in general of all unitary matrices that map the multiqudit Pauli group onto itself. In the case of a single qubit this amounts to $|\mathcal{C}(2)| = 24$ elements, which can be generated from the Hadamard gate H and the phase gate $S = e^{i(\pi/4)\sigma_z}$.

Now, noting that the second power of the correlation function (3) is a polynomial of degree 2 in the entries of the local random unitary matrices $U_n \in \mathrm{U}(d)$ and their complex conjugates allows us to replace the average over the local unitary groups $\mathrm{U}(d)$ in Eq. (4) with an average over all elements of the respective Clifford groups $\mathcal{C}(d)$, yielding

$$\mathcal{R}_A^{(2)} = \frac{1}{|\mathcal{C}(d)|^{|A|}} \sum_{\alpha_1,\dots,\alpha_k=1}^{|\mathcal{C}(d)|} \left\langle \mathcal{O}_{U_{\alpha_1}}^{(i_1)} \cdots \mathcal{O}_{U_{\alpha_k}}^{(i_k)} \right\rangle^2. \quad (14)$$

Equation (14) is a general formula that allows one to calculate the second moment for general local dimension d and arbitrary subsystems A. If one is interested in the specific case of systems of qubits, i.e., $d = 2$, we can further use that the Clifford group has the property to map the multiqubit Pauli group onto itself and thus each of the observables $\mathcal{O}_{U_\alpha}^{(i)}$ becomes equal to $\pm\sigma_\alpha^{(i)}$, where $\sigma_\alpha^{(i)}$ denotes the αth Pauli matrix acting on qubit i of the total N-qubit system. All in all, Eq. (14) thus simplifies to a sum over the squared elements of the correlations tensors $T_{\alpha_1,\dots,\alpha_k}^{(A)} = \langle \sigma_{\alpha_1}^{(i_1)}, \dots, \sigma_{\alpha_k}^{(i_k)} \rangle$, leading to

$$\mathcal{R}_A^{(2)} = \frac{1}{3^{|A|}} \sum_{\alpha_1,\dots,\alpha_k=1}^{3} \left(T_{\alpha_1,\dots,\alpha_k}^{(A)} \right)^2. \quad (15)$$

Hence, in order to determine the moments $\mathcal{R}_A^{(2)}$ exactly it suffices to measure all elements of the correlation tensors $T^{(A)}$ which can be directly extracted from the full correlation tensor $T_{\alpha_1,\dots,\alpha_N} = \langle \sigma_{\alpha_1} \otimes \cdots \otimes \sigma_{\alpha_N} \rangle$, with $\alpha_j = x, y, z$, which consists of 3^N elements.

In conclusion, as the pure state concurrence (8) and the corresponding lower bound (12) are simple functions of the second moments $\mathcal{R}_A^{(2)}$, we can use Eq. (15) to measure them directly using 3^N measurement settings. Such a direct measurement, however, becomes impractical as soon as one reaches system sizes of several tens of qubits where, due to the exponential scaling 3^N, the required number measurements becomes too large. In the latter regime it can be favorable to estimate the concurrence approximately using randomized measurements at the expense of a nonzero statistical error. In the next section we will analyze this statistical error and discuss the scaling of the required number of measurement settings, as well as the required number of projective measurements per individual measurement setting, in order to reach an estimate with a predefined accuracy.

III. STATISTICAL ESTIMATION OF THE MULTIPARTICLE CONCURRENCE

A. Unbiased estimators of Eqs. (7) and (11)

In experiments randomized measurement protocols can only be realized with finite samples of measurements. Consequently, an estimation of the randomized population probabilities contained in Eqs. (7) and (11), i.e., $\mathbb{E}_U[P_U^2(s)]$ and $\mathbb{E}_U[P_U(s)P_U(s')]$, will involve a finite statistical error.

Furthermore, in practice one also needs to estimate the population probabilities $P_U(s)$ based on finitely many rounds of projective measurements.

In the following we will assume that one round of randomized measurements consists of a sample of M random measurement bases, each of which undergoes a finite number K of projective measurements. The latter allow us to estimate the $P_U(s)$, its second powers $P_U^2(s)$, as well as cross terms of the form $P_U(s)P_U(s')$ for each individual choice of random measurement bases defined by the local unitary transformation $U = U_1 \otimes \cdots \otimes U_N$. In order to do so we first introduce an unbiased estimator of the population probability $P_U(s)$, which reads $\tilde{P}_U(s) = Y(s)/K$, where $Y(s)$ denotes a random variable distributed according to the multinomial distribution defined by the distribution $\{P_U(s)\}_s$ with K independent trials. Given $\tilde{P}_U(s)$, it is straightforward to derive appropriate estimators for its monomials (see Appendix B 1 for details), yielding

$$\tilde{P}_U^{(2)}(s) = \frac{\tilde{P}(s)[K\tilde{P}(s) - 1]}{K - 1}, \quad (16)$$

$$\tilde{P}_{U_i}^{(1,1)}(s, s') = \frac{K}{K - 1} \tilde{P}(s)\tilde{P}(s'). \quad (17)$$

Given this set of unbiased estimators of the involved population probabilities, we can go one step further and introduce statistically sound estimators of the relevant quantities contained in Eqs. (7) and (11), namely, $\mathbb{E}_U[P_U^2(s)]$ and $\mathbb{E}_U[P_U(s)P_U(s')]$, leading to

$$\overline{P_U^2(s)} = \frac{1}{M} \sum_{i=1}^{M} \tilde{P}_{U_i}^{(2)}(s), \quad (18)$$

$$\overline{P_U(s)P_U(s')} = \frac{1}{M} \sum_{i=1}^{M} \tilde{P}_{U_i}^{(1,1)}(s, s'). \quad (19)$$

The estimators (18) and (19) thus reflect the fluctuations resulting from both finite M and K leading to a nonzero statistical error. In order to determine the latter, different strategies can be pursued, one of which consists in a straightforward statistical approach exploiting the measurement data produced form either real or numerical experiments (see Fig. 2). In this way it is possible to investigate the statistical error of the involved estimators for systems of limited size and for specific targeted quantum states [28–31]; however, it is in general not possible to extrapolate the statistical effects to systems consisting of larger particle number. Alternatively, one can evaluate the statistical error analytically based on the given properties of the estimators' distributions, an approach that we will pursue further in Sec. III B.

Before moving on to the analysis of the statistical errors of Eqs. (18) and (19) we note that the squared averaged population probability $\mathbb{E}_U[P_U^2(s)]$ no longer depends on the bit string s. Hence, when estimating $\mathbb{E}_U[P_U^2(s)]$ it can be advantageous to consider an unbiased estimator that includes also an average over the subsets $I \subset \{0, 1\}^N$ of observed bit strings s. For instance, instead of Eq. (18) we can use

$$\tilde{X} = \frac{1}{|I|M} \sum_{s \in I} \sum_{i=1}^{M} \tilde{P}_{U_i}^{(2)}(s), \quad (20)$$
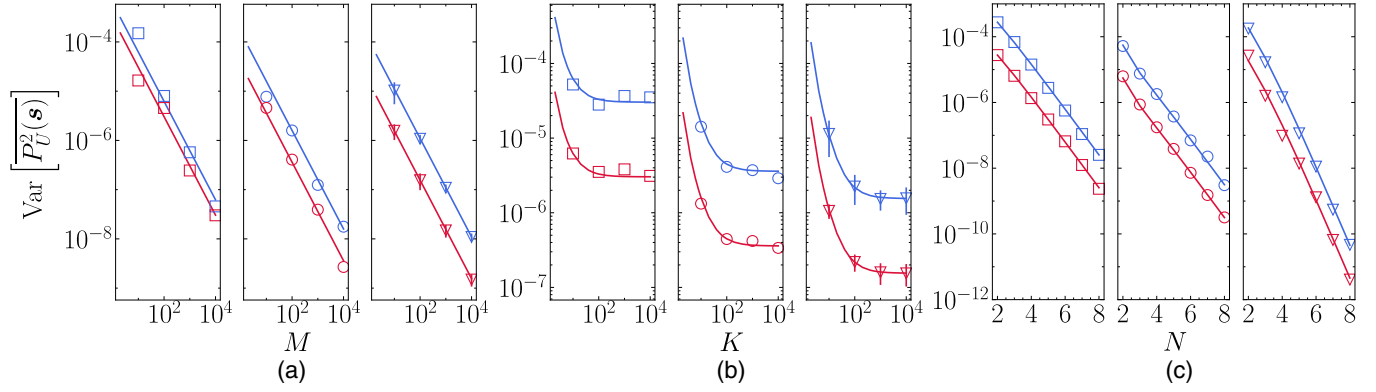
FIG. 2. (a) Plot of the variance of the estimator of the squared population probabilities for five qubits as a function of the number M of sampled local measurement bases, with $K = 10$ (upper blue circles) and $K = 10^2$ (lower red circles). The left plot corresponds to a random product state, the middle one to the GHZ state, and the right plot to a Haar random state. For the latter, the error bar marks the standard deviation of 100 averaged Haar random states. Solid lines correspond to the analytical result obtained via an exact average with respect to the Haar measure. (b) Plot of the same variance as a function of the number of projective measurements K with $M = 10$ and 10^2. (c) Plot of the same variance as a function of the number N of qubits with $M = 10^2$ and 10^3.

which is also an unbiased estimator for the squared averaged population probability $\mathbb{E}_U[P_U^2(s)] = \mathbb{E}_{\text{multi},U}[\tilde{X}]$. This procedure is particularly relevant for an increasing number of qubits N, in which case the probability of observing one particular bit string can become vanishingly small.

B. Analysis of the statistical errors

In order to analyze the statistical error of the estimators (18)–(20) we first have to evaluate their respective variances. For instance, in the case of Eq. (18) this yields

$$\text{Var}[\overline{P_U^2(s)}] = \frac{1}{M^2} \sum_{i=1}^{M} \text{Var}[\tilde{P}_{U_i}^{(2)}(s)], \qquad (21)$$

with

$$\text{Var}[\tilde{P}_{U_i}^{(2)}(s)] = \frac{1}{(K-1)^2} \{(5 - 3K)\mathbb{E}_U[P_U^4(s)]$$
$$+ 4(K-2)\mathbb{E}_U[P_U^3(s)] + 2\mathbb{E}_U[P_U^2(s)]\}, \qquad (22)$$

which shows that the underlying error depends on the higher-order randomized population probabilities $\mathbb{E}_U[P_U^2(s)]$, $\mathbb{E}_U[P_U^3(s)]$, and $\mathbb{E}_U[P_U^4(s)]$, which in turn are independent of the choice of the bit string s. In Fig. 2 we present a comparison between the numerically and analytically estimated values of the variance (21) for a number of exemplary quantum states (see Appendix B 1 for details on the calculations). We find that the variance decays for all states inversely with M, as expected from the central-limit theorem, while its dependence on K reaches a plateau after an initial decay. All in all, we find that the numerical results agree very well with the analytical predictions also for varying number of qubits [see Fig. 2(c)].

In Fig. 3 we present similar results for the estimator (19). Note that in this case the symbolic expression of the respective variance [see Eq. (B12) in Appendix B 1] is more complicated as it depends on the cross terms $\mathbb{E}_U[P_U^t(s)P_U^k(s')]$, with $t, k = 1, 2$, which themselves depend on the Hamming

distance $D(s, s')$. For this reason, we calculate the variance for all values of s and s' and present the average over the respective values in Fig. 3. As for the variance of Eq. (18), we find good agreement with the analytical predictions for the states under consideration.

Given the analytical expression of the variance (21), it is straightforward to derive a confidence interval for the estimators (18) and (19) for the target state under consideration and a given number of measurements M and K. To do so, we use the two-sided Cantelli inequality (see Refs. [63]), yielding

$$\text{Pr}[|\overline{P_U^2(s)} - \mathbb{E}[P_U^2(s)]| \geqslant \delta] \leqslant \frac{2\,\text{Var}[\tilde{P}_{U_i}^{(2)}(s)]}{\text{Var}[\tilde{P}_{U_i}^{(2)}(s)] + \delta^2}, \quad (23)$$

which, by requiring that the confidence $1 - \text{Prob}(|\tilde{\mathcal{R}}^{(t)} - \mathcal{R}^{(t)}| \geqslant \delta)$ of this estimation is at least γ, leads to the following minimal two-sided error bar:

$$\delta_{\text{err}} = \sqrt{\frac{1+\gamma}{1-\gamma}\text{Var}[\tilde{P}_{U_i}^{(2)}(s)]}. \qquad (24)$$

In order to do the final step of deriving a suitable error bar on the estimate of the concurrence, we have to propagate the respective error (24) through the square root contained in the expression (7). This can be done up to first order in δ_{err} using the standard rule for the propagation of uncertainties, leading to

$$\delta_C = \frac{\partial C}{\partial \mathbb{E}_U[P_U^2(s)]}\delta_{\text{err}} + O(\delta_{\text{err}}^2). \qquad (25)$$

Now we are in the position to determine the required number of measurements MK as well as their ratio M/K in order to estimate the concurrence up to an error of δ_C. To do so, we fix a desired relative error of 10% for the concurrence and determine the optimal values of M and K such that δ_C fulfills this error requirement. In practice, this is done by analytically evaluating δ_C for a number of values of M and K chosen from the range of values $10^1, \ldots, 10^{16}$. In Fig. 4
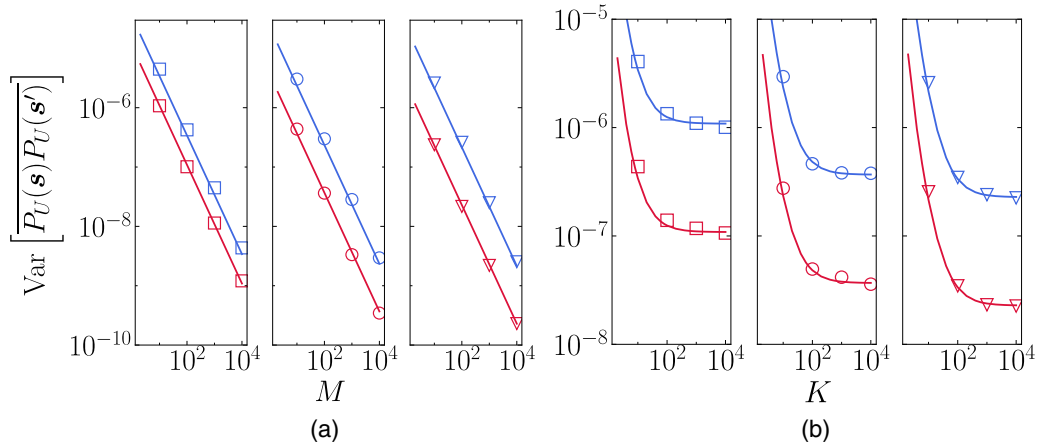
FIG. 3. (a) Plot of the variance of the estimator (19) for five qubits averaged over all combinations of s and s' and as a function of the number M of sampled local measurement bases with $K = 10$ (upper blue circles) and $K = 10^2$ (lower red circles). The left plot corresponds to a random product state, the middle one to the GHZ state, and the right plot to a Haar random state. Solid lines correspond to the analytical result obtained via an exact average with respect to the Haar measure. (b) Plot of the same variance as a function of the number of projective measurements K with $M = 10$ and 10^2.

we present the results of this procedure as a function of the number N of involved qubits. Note that this can be done efficiently due to the analytical estimates of the variance (21) and can, in principle, be carried out for an arbitrary number N
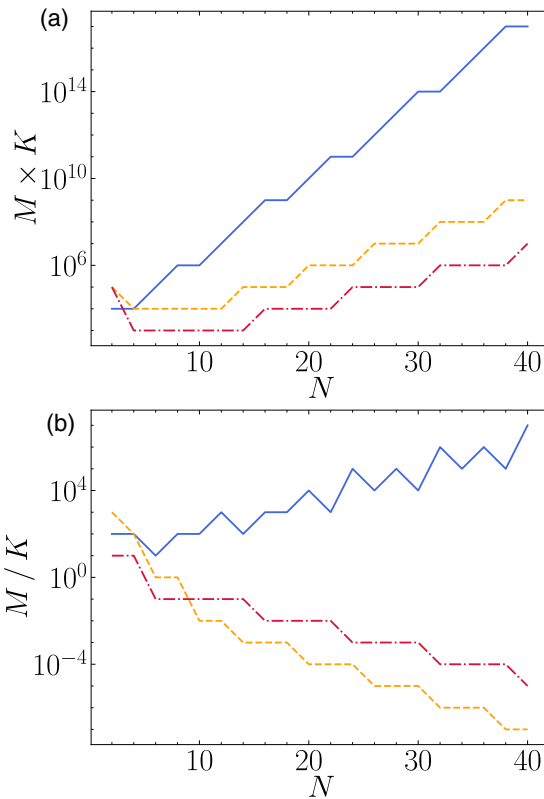

FIG. 4. Plot of (a) the total number of measurements MK and (b) the corresponding optimal ratio M/K required for an estimation of the concurrence with a relative error of at most 10% as a function of the number of qubits for a GHZ state (blue solid line) and a Haar random state (yellow dashed line). The red dash-dotted line shows the respective results for the estimation of the concurrence of a Haar random state using the estimator (20).

of qubits. Previous studies of this type focusing on estimations of the purity were bounded to values of $N \leqslant 10$ as they relied on numerical estimates of the underlying statistical errors [28–31].

We also note that the exact analytical assessment of the statistical error of the estimator (20) is more involved because the sum over s leads to many cross terms in the respective variance. However, in the particular case of Haar random states we can circumvent this problem because correlations between different bit strings of Haar random states are with increasing N exponentially suppressed [64,65]. Making use of this fact allows us to evaluate the underlying variance and obtain an estimate of the respective statistical error (see Appendix B 1 for details). As an example we included the results of the latter calculation in Fig. 3, showing that it can lead to an improvement as long as the dimension of the overall Hilbert space is small compared to the number K of individual projective measurements per random measurement setting.

IV. APPLICATIONS TO TYPICAL MULTIPARTICLE ENTANGLED STATES

Having analyzed in detail the measurement resources required for the evaluation of Eqs. (7) and (11) in the preceding section, we move on and investigate how the introduced randomized measurement protocol performs in practice. In this respect, we use the methods introduced in Sec. II in order to characterize the multiparticle entanglement properties of examples of typical multiparticle entangled states and investigate the observed performance in the presence of noise in the form of gate errors.

A. Analytical results for pure states

To begin with, we will summarize some important analytical expressions of the concurrence for several examples of multiparticle states and discuss their respective asymptotic behavior in the limit of large particle numbers. We note

that the analytical expressions for the concurrence of pure Greenberger-Horne-Zeilinger (GHZ) states of N qubits can be easily derived from the fact that all its reduced states are maximally mixed states of rank 2 and thus have a purity of $\frac{1}{2}$ [47,48], leading to

$$C_N(|\text{GHZ}_N\rangle) = 2^{1-N/2}\sqrt{2^{N-1}-1}, \qquad (26)$$

which yields $\sqrt{2}$ in the limit $N \to \infty$.

Furthermore, we derive in the following also an analytical expression for the concurrence of Haar random pure states of N qubits. In order to do so we first note that a pure Haar random state reads $|\psi\rangle = U|0\rangle^{\otimes N}$, with $U \in \text{U}(2^N)$ picked uniformly according to the Haar measure. Hence, the resulting concurrence of the output state is a polynomial functions of the unitary transformation U whose average over the unitary group can be evaluated using the well-known expression

$$\int_{\text{U}(d)} U_{i_1,j_1} \cdots U_{i_t,j_t} U^*_{\tilde{i}_1,\tilde{j}_1} \cdots U^*_{\tilde{i}_t,\tilde{j}_t} dU$$

$$= \sum_{\pi,\sigma \in S_t} \delta_{i_1,\tilde{i}_{\pi(1)}} \cdots \delta_{i_t,\tilde{i}_{\pi(t)}} \delta_{j_1,\tilde{j}_{\sigma(1)}} \cdots \delta_{j_t,\tilde{j}_{\sigma(t)}} \text{Wg}_d(\pi^{-1}\sigma), \qquad (27)$$

where the sum runs over the elements of the symmetric group S_t and Wg_d denotes the so-called Weingarten function which depends on the structure of the permutation $\pi^{-1}\sigma$ and the dimension d [66,67]. Doing so with the square of the concurrence (7) leads to the expression

$$\mathbb{E}_\psi[C_N(\psi)^2] = 4 - \frac{8(1+d)^N}{2^N(1+d^N)}, \qquad (28)$$

where we used the notation $\mathbb{E}_\psi[\cdots]$ to denote the analytical average over U and thus over the Haar random state $|\psi\rangle$. We emphasize that the square root of Eq. (28) provides also a good approximation of the average $\mathbb{E}_\psi[C_N(\psi)]$ already for moderate numbers of N due to the concentration of the concurrence around its mean value (see Fig. 5). The latter is a direct consequence of the concentration of measure phenomena occurring for samples of Haar random quantum states in Hilbert space of growing dimension [68,69].

Using Eq. (28), we find that the average concurrence for Haar random multiqubit states converges to 2 if the number of qubits N goes to infinity. Hence, while GHZ states yield a larger concurrence for small qubit numbers, i.e., $N = 2, 3, 4$, the concurrence of Haar random states generally increases faster for large qubit numbers and finally also reaches a larger asymptotic value $C_\infty(|\text{Haar}_\infty\rangle) > C_\infty(|\text{GHZ}_\infty\rangle)$. Finally, the question remains whether 2 is also the global maximum of the concurrence in the limit $N \to \infty$. To answer this question we make the hypothetical assumption that all subsystems of a pure N-qudit state are maximally mixed and thus all the corresponding purities contained in Eq. (6) become minimal. Hence, we find that all the purities are equal to $1/d_A$, where d_A denotes the dimension of the respective subsystem under consideration. In the case of a system of qubits we thus have $d_A = 2^{|A|}$ and summing over all possible subsystems leads to
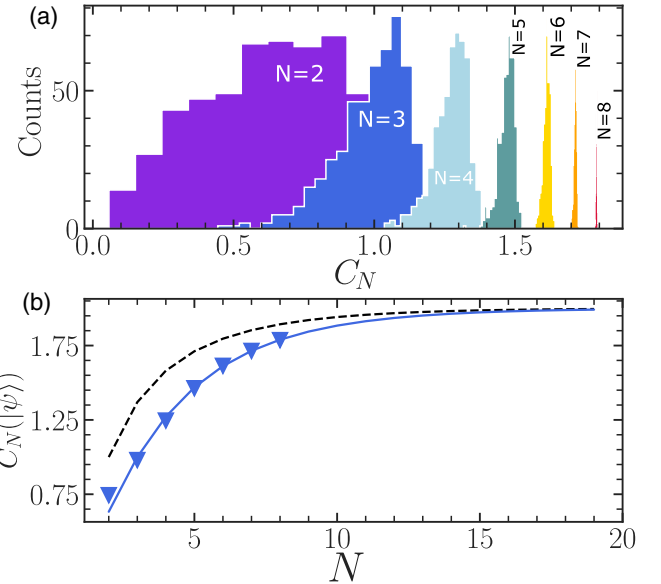

FIG. 5. (a) Histogram of the values of the multiparticle concurrence (6) evaluated for samples of 10^3 Haar random states for $N = 2$ (violet, left) to $N = 8$ (red, right) qubits. (b) Plot of the mean values associated with the distributions presented above as a function of the number of qubits N (blue triangles). As a comparison, the analytical law (28) for the mean value of the concurrence for Haar random states is shown (blue solid line), as well as the overall upper bound of the maximum of the concurrence presented in Eq. (29) (black dashed line).

the formula

$$2\sqrt{1 - \frac{1}{2^N} - \sum_{k=0}^{N-1} \frac{\binom{N}{k}}{2^{N+k}}} = 2^{1-N}\sqrt{1 + 4^N - 2^N - 3^N}, \quad (29)$$

which provides an upper bound of the global maximum of the concurrence (6). Note that the asymptotic value of Eq. (29) in the limit $N \to \infty$ is also 2, while for each finite N it is strictly larger than Eq. (28).

B. Influence of noise on multiparticle entanglement

Given the statistical analysis of the required measurement resources for an estimation of the multiparticle concurrence (7), we are now in the position to apply these insights in practice. We first do so in the case of pure GHZ as well as Haar random states and compare the results to the analytical expressions presented in Sec. IV A. Figures 6(a) and 6(b) present numerical estimates of the concurrence with the measurement resources M and K chosen in such a way that the resulting statistical errors remain below 10% and 5% of the absolute value of the concurrence, respectively. While the fluctuations of the resulting estimates are apparent, one clearly observes that they remain below the anticipated relative error bounds of 10% and 5%.

In a further analysis we estimate the lower bound of the multiparticle concurrence of noisy versions of the respective pure states with randomized measurements using Eq (11). In order to stay close to experimental implementations using noisy intermediate-scale quantum (NISQ) devices, we
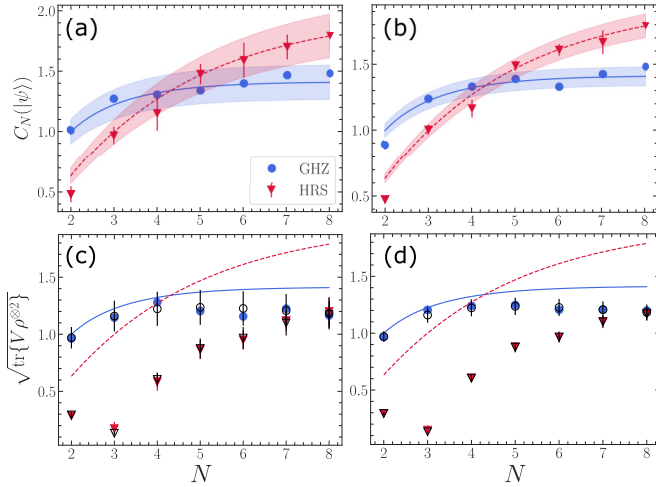
FIG. 6. Numerical estimation of (a) and (b) the multiparticle concurrence (7) and (c) and (d) its lower bound (11) of GHZ states (blue circles) and Haar random states (red triangles) as a function of the number of qubits N. The values of M and K are chosen in order to reach a relative error of (a) 10% and (b) 5% according to the analysis presented in Sec. III. While solid and dashed lines present the corresponding analytical predictions for pure states, black circles and triangles indicate the respective true values of the concurrence's lower bound obtained via Eq. (9). Note that red triangles and the corresponding error bars have been obtained from samples of 30 Haar random states. Also shown are the noise-prone cases where the states are produced by a quantum circuits consisting of single- and two-qubit gates inflicted with local depolarizing errors of (c) 0.01% and (d) 0.1%. In order to approximate mixed Haar random states, we used random quantum circuits containing 500 randomly sampled gates from a universal gate set (see Fig. 1 and Sec. V).

produce the respective GHZ and Haar random states with simulated quantum circuits consisting of series of single- and two-qubit gates for which we assume local depolarizing errors with error probabilities ε_1 and ε_2, respectively. However, if the latter are chosen too large, the resulting output states will be considerably mixed and the associated lower bound of the concurrence very small or even zero. Hence, in order to produce states with a reasonable fidelity, i.e., such that the lower bound of the concurrence is above zero, the magnitude of ε_1 and ε_2 should not be to large. We can roughly estimate the resulting fidelities of the final output states by summing up the effects of all single- and two-qubit gate errors as $\epsilon = 1 - (1 - \varepsilon_1)^{\#_{1\text{-qu}}}(1 - \varepsilon_2)^{\#_{2\text{-qu}}}$, where $\#_{1\text{-qu}}$ and $\#_{2\text{-qu}}$ denote the total numbers of applied single- and two-qubit gates, respectively. The estimated overall accumulated error when producing GHZ states of N qubits is thus given by $1 - (1 - \varepsilon_1)(1 - \varepsilon_2)^{N-1}$ as it requires the application of exactly $N - 1$ controlled-NOT (CNOT) gates and only a single Hadamard gate. Hence, the number of required two-qubit gates grows linearly with the number of involved qubits and the overall accumulated error remains below 10% even for two-qubit gate errors of about 1%.

The Haar random states, however, can only be approximated by a series of gates that are chosen randomly from a universal set of gates (in Sec. V A we discuss one possible way of doing so) and thus one has to find a tradeoff between the

required randomness one wants to achieve and the total error inflicted by the executed gate operations. If we assume that the latter circuits consist of overall n_{gates}, with twice as many single- as two-qubit gates, we accumulate an overall error of $1 - (1 - \varepsilon_1)^{n_{\text{gates}}2/3}(1 - \varepsilon_2)^{n_{\text{gates}}/3}$. Furthermore, we need to apply at least $n_{\text{gates}} > 500$ gates in order to reach a sufficient amount of randomness in the case of $N = 9$ qubits. Taking these competing factors into account, we estimate that for the errors $\varepsilon_1 = 0.01\%$ and $\varepsilon_2 = 0.1\%$ the overall accumulated error does not exceed 20% and thus a reasonable fidelity of the respective Haar random state is reached.

We thus simulated the respective circuits with the above error rates and estimated the concurrence using Eq. (11). The results are presented in Figs. 6(c) and 6(d). Note that for the simulation of Eq. (11) in Figs. 6(c) and 6(d) we used the same measurement numbers M and K that have been used for the respective pure states in order to reach relative errors of 10% and 5%, respectively. Even though this is only a rough estimate, the obtained results agree well with the exact values of the concurrence's lower bound (9), which are also depicted in Fig. 6. Motivated by this result, we move on and apply the respective protocols for estimating the concurrence other multiparticle entangled states produced by different classes of random quantum circuits.

V. APPLICATIONS TO THE CHARACTERIZATION OF RANDOM QUANTUM CIRCUITS

A. Random quantum circuits

In the following we consider quantum circuits which are defined through sequences of unitary gates that are drawn randomly from a predetermined gate set $\mathcal{I}$ and applied to randomly selected subsets of qubits (see Fig. 1 and 7). In particular, we prepare the initial state of the N qubits in the ground state $|0\rangle^{\otimes N}$ and apply exactly T randomly drawn gates, i.e., T can be considered as a discrete-time parameter which also denotes the total count of quantum gates that have been applied. Note that selection of gates from the set $\mathcal{I}$ as well as the choice of qubits to which they are applied is entirely random. The N-qubit output state of such a random quantum circuits consequently depends on the number of applied gate operations T and the properties of the gate set $\mathcal{I}$ under consideration. We will regard three distinct types of gate sets which have fundamentally different properties concerning their universality and classical simulability and study the entanglement that is produced by them.

With the goal of performing universal quantum computation in mind, one usually considers universal gate sets, i.e., sets which allow one to approximate any N-qubit unitary transformation with arbitrary precision ϵ [1]. One of the most famous universal gate sets consists of the two-qubit CNOT gate C_X, the Hadamard gate H, and the $T = \exp(-i\sigma_z\pi/8)$ gate and we refer to it in the following as $\mathcal{I}_{\text{uni}}$ [1] (see Fig. 1). A random quantum circuit consisting of gates from $\mathcal{I}_{\text{uni}}$ is expected to approximate an overall Haar random unitary transformation over N qubits once a threshold time T^* is reached. The universal gate set $\mathcal{I}_{\text{uni}}$ has also been used to approximate Haar random states in Sec. IV. Also note that noisy variants of such universal random circuits are at the
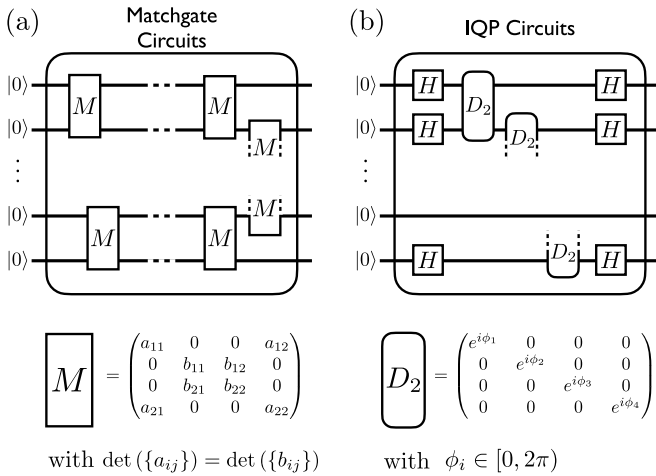
FIG. 7. Representation of (a) matchgate and (b) IQP circuits together with the matrix representation of the native gate operations M and D_2, respectively. The table summarizes the properties of the types of random quantum circuits considered. The second column indicates whether the respective gate set gives rise to universal quantum computations. The third column summarizes the complexity of the circuits showing whether or not the circuit is classically simulatable and under which conditions. Strong and weak indicate whether it is possible to classically simulate the circuits output probabilities or to classically sample from it, respectively. One and many say whether the task involves a single qubit or many qubits.

FIG. 8. Numerical estimation of (a) and (b) the multiparticle concurrence (7) and (c) and (d) its lower bound (11) of output states of random IQP (green pentagons) and MG (orange diamonds) circuits. The noiseless cases with (a) M and (b) K are chosen in order to reach a relative error of (a) and (c) 10% and (b) and (d) 5% according to the analysis for Haar random states presented in Sec. III. The IQP circuits consist of $N(N-1)/2$ diagonal gates and the MG circuits of 150 randomly sampled nearest-neighbor matchgates. Error bars are obtained by resampling the respective states 30 times. Also shown are (c) and (d) the cases where we assumed that each two-qubit gate used to produce the respective states has a local depolarizing error of 0.1%. Black symbols indicate the respective true values of the concurrence's lower bound obtained via Eq. (9).

heart of the first demonstrations of quantum computational advantages based on cross-entropy benchmarking [3].

In the following we will investigate the entanglement properties of other so-called restricted classes of quantum circuits, i.e., circuits produced by gate sets that are in general not universal. A famous example of such a restricted class of quantum circuits is that consisting of so-called Clifford transformations which are generated by the set $\mathcal{I}_{\mathrm{Clif}} = \{C_X, H, P = \exp(-i\sigma_z\pi/4)\}$. The latter are, by virtue of the Gottesman-Knill theorem, always classically simulatable when initiated in the state $|0\rangle^{\otimes N}$ and read out in the computational basis [1]. Another class of quantum circuits that is known to be efficiently simulatable are so-called nearest-neighbor matchgate circuits [see Fig. 7(a)]. Matchgates are two-qubit gates that consist of two single-qubit gates with equal determinants that act on the even- and odd-parity subspace of the two qubits, respectively [70,71]. Matchgate (MG) circuits on N qubits have also been shown to be equivalent to a system of non-interacting fermions in one dimension which is governed by interactions of at most quadratic order in the fermion creation and annihilation operators [72]. In the random circuit model we generate in each time step a random matchgate and apply it to a random pair of nearest-neighbor qubits. Lifting the nearest-neighbor restriction of matchgates circuits promotes them to the realm of universal for quantum computation [70].
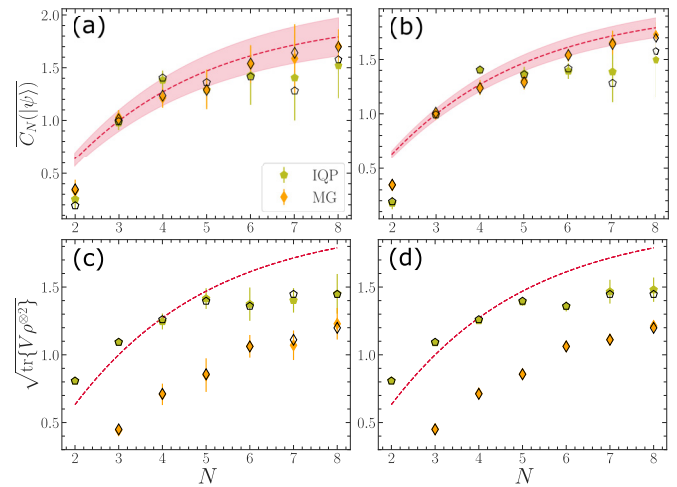
Finally, we consider the class of commuting quantum circuits which are made up of gates diagonal in the computational basis [see Fig. 8(b)]. The latter become nontrivial if the qubits are initiated and read out in local bases that are orthogonal to the computational bases, e.g., $\{|x_i\rangle^{\otimes N}\}_{i=1}^N$, with $x_i = \pm$. Due to the commuting property of the diagonal gates, there is not a natural time ordering of gates for a given circuit and thus the resulting class of circuits is referred to as instantaneous quantum polynomial-time (IQP) circuits. The IQP circuits do not allow for universal quantum computation but they are known to be in general hard to simulate classically [73,74]. Specific designs of IQP circuits deal with diagonal gates of the form $W_r = \mathrm{diag}\{e^{i\phi_1}, \ldots, e^{i\phi_{2^r}}\}$, with independent and uniformly sampled $\phi_i \in [0, 2\pi)$, which act on a subset of r qubits and are applied to all combinations of r qubits in random order [75,76]. In particular, we will consider IQP circuits with $r = 2$ which consist of precisely $N(N-1)/2$ diagonal gates. For the former type, i.e., $r = 2$, a restriction to gates acting only on nearest-neighbor qubits once again makes the circuits classically simulatable [77].

B. Numerical results

As a last application we use three of the aforementioned random circuits to test our randomized measurement protocols on further examples of multiparticle entangled states. So far, we have considered random circuits consisting of the universal gate set $I_{\mathrm{uni}} = \{H, T, C_X\}$ in order to approximate Haar random states (see Sec. IV B). Here we focus on two

examples of random circuits produced by restricted gates sets, i.e., nearest-neighbor matchgates and IQP circuits (see Fig. 7). The corresponding gate sets I_{MG} and I_{IQP} are nonuniversal and also classically simulatable but in some cases can produce more entanglement than the aforementioned universal set I_{uni}, for which reason they provide an appropriate test case for our randomized measurement protocol.

We start by the noiseless cases presented in Figs. 8(a) and 8(b), where we estimated the concurrence of samples of output states of the above-mentioned random circuits. To do so, we used in all three cases the same measurement resources M and K as determined for Haar random states of the same number of qubits. We find that even though I_{MG} and I_{IQP} produce very different ensembles of states, the resulting concurrence agrees well, i.e., within one standard deviation, with the respective analytically determined values using Eq. (6). However, we find that I_{MG} and I_{IQP} circuits lead in general to larger fluctuations of the concurrence as compared to I_{uni}. Note that the former have been analyzed by resampling the concurrence of the corresponding random circuit 100 times in order to numerically determine the underlying standard deviation, as shown in Fig. 8.

Finally, we consider the same random circuits but with error-prone gates simulated by additional local depolarizing channels with the same single- and two-qubit error probabilities as used also in Sec. IV B, i.e., $\varepsilon_1 = 0.01\%$ and $\varepsilon_2 = 0.1\%$. The results for estimating the concurrence's lower bound of the respective output states are presented in Figs. 8(c) and 8(d). Again we find that using the same measurement resources as for the corresponding noiseless cases, one achieves good agreement with the corresponding exact values. However, in comparison to the noiseless cases, the resulting estimates do not fluctuate more, which might be explained by the increased mixing of local subsystems. The more the one-qubit reduced states are mixed the less they fluctuate over the local unitary ensembles while performing randomized measurements on them. Hence, this indicates that protocols based on randomized measurements might be relevant candidates for characterization of entanglement in close to random, noisy quantum circuits in the intermediate regime.

VI. CONCLUSION

In this article we investigated how to estimate the entanglement content, as measured by the multiparticle concurrence, of many-body quantum systems employing protocols based on randomized measurements. We formulated schemes for measuring the multiparticle concurrence of pure states as well as a corresponding lower bound in the case of mixed states. In addition, we analyzed in detail the occurring statistical error when estimating the involved quantities with appropriate unbiased estimators and derived exact scaling laws of the required measurement resources for estimating the concurrence of an important subclass of multiparticle entangled states.

We demonstrated the introduced protocols by numerically analyzing the multiparticle concurrence of the aforementioned class of quantum states as well as for ensembles of output states of different classes of random quantum circuits, such as matchgate and IQP circuits. Finally, we investigated the influence of noise in terms of single- and two-qubit gate

errors on the multiparticle entanglement of the states under consideration and thereby showed that the obtained results on the required measurement resources prove useful in the noisy intermediate-scale regime. However, we also show that the required measurement resources strongly depend on the underlying class of quantum states under consideration, showing that a detailed statistical analysis was justified.

All in all, the outlined randomized measurement protocols are promising tools for the analysis of multiparticle entanglement in NISQ devices. Nevertheless, the measurement resources required for an estimation of the concurrence with a reasonably small statistical error increase quickly when reaching regimes of large particles numbers, i.e., beyond $N \approx 30$, rendering the presented protocols impractical. Hence, while moving towards larger and larger particle numbers of NISQ devices with improved quality one has to develop alternative tools that deal with the aforementioned problem. A possible solution in this direction is to exploit more information about the actual quantum states under investigation, e.g., the fact that they are likely contained in a subspace of limited qubit excitations or entanglement content. Alternatively, one might employ more involved nonlocal measurement schemes on an extended Hilbert space [48,51] in order to analyze its multiparticle entanglement in a more efficient manner.

APPENDIX A: MULTIPARTICLE CONCURRENCE FROM RANDOMIZED MEASUREMENTS

1. Derivation of Eqs. (7) and (11)

The concurrence of a pure N-qudit state $|\psi\rangle \in \mathbb{C}^d$ is defined as [47,48]

$$C_N(|\psi\rangle) = 2\sqrt{1 - \frac{1}{2^N} \sum_{A \subseteq \{1,\ldots,N\}} \text{tr}(\varrho_A^2)}, \quad \text{(A1)}$$

where $\varrho_A = \text{tr}_{\bar{A}}(|\psi\rangle\langle\psi|)$, with $\bar{A} = \{1,\ldots,N\} \setminus A$, denotes the reduced density matrix of the pure state $|\psi\rangle$ with respect to the subsystem associated with the subset $A \in \{1,\ldots,N\}$. Note that the sum in Eq. (A1) runs over all subsets including the empty set for which we have $\varrho_\emptyset = 1$. In the following we will show that one can evaluate Eq. (A1) using locally randomized measurements. To do so, we regard the population probabilities

$$P_U(\boldsymbol{s}) = \text{tr}(U\varrho U^\dagger |\boldsymbol{s}\rangle\langle\boldsymbol{s}|), \quad \text{(A2)}$$

where $|\boldsymbol{s}\rangle = |s_1,\ldots,s_N\rangle$, with $s_i = 1\ldots d$, denotes an arbitrary element of the computational basis of N qudits and $U = U_1 \otimes \cdots \otimes U_N$, with $U_i \in \text{U}(d)$, a randomly drawn local unitary transformation. Further, upon averaging the square of Eq. (A2) over the U's with respect to the local Haar measure

on each of the individual qudit subspaces we find

$$
\begin{aligned}
\mathbb{E}_U[P_U(\boldsymbol{s})^2] &= \mathbb{E}_U[\mathrm{tr}(\varrho U|\boldsymbol{s}\rangle\langle\boldsymbol{s}|U^\dagger)^2] \\
&= \mathrm{tr}\{\varrho^{\otimes 2}\mathbb{E}_U[(U|\boldsymbol{s}\rangle\langle\boldsymbol{s}|U^\dagger)^{\otimes 2}]\} \\
&= \mathrm{tr}\left(\varrho^{\otimes 2}\bigotimes_{i=1}^{N}\mathbb{E}_{U_i}[U_i^{\otimes 2}|s_i\rangle\langle s_i|^{\otimes 2}U_i^{\dagger\otimes 2}]\right) \\
&= \left(\frac{D_d^{(2)}}{2}\right)^N \mathrm{tr}[\varrho^{\otimes 2}(P_+\otimes\ldots\otimes P_+)].
\end{aligned}
\tag{A3}
$$

In the last line of Eq. (A3) we used for $t=2$ the relation

$$
\mathbb{E}_{U(d)}[U^{\otimes t}|s\rangle\langle s|^{\otimes t}U^{\dagger\otimes t}] = D_d^{(t)}P_+,
\tag{A4}
$$

where P_+ denotes the projector on the symmetric subspace of $(\mathbb{C}^d)^{\otimes t}$ and $D_d^{(t)} = t!(d-1)!/(t+d-1)!$ the inverse of its dimension. For $t=2$ we can write $P_+ = (\mathbb{1}+S)/2$, where S denotes the SWAP operator on $(\mathbb{C}^d)^{\otimes 2}$. Using the latter and the fact that $\mathrm{tr}(S\varrho^{\otimes 2}) = \mathrm{tr}(\varrho^2)$ in Eq. (A3) allows us to arrive at the expression

$$
\begin{aligned}
\overline{P(\boldsymbol{s})^2} &= \left(\frac{D_d^{(2)}}{2}\right)^N \mathrm{tr}\left(\prod_{i=1}^{N}(S_i+\mathbb{1})\varrho^{\otimes 2}\right) \\
&= \left(\frac{D_d^{(2)}}{2}\right)^N \sum_\alpha \mathrm{tr}\varrho_\alpha^2
\end{aligned}
\tag{A5}
$$

and thus shows that the concurrence (A1) can be expressed as

$$
C_N(|\psi\rangle) = 2\sqrt{1 - \frac{d^N(d+1)^N}{4^N}\sum_{\boldsymbol{s}\in\{0,1\}^N}\mathbb{E}_U[P_U^2(\boldsymbol{s})]}.
\tag{A6}
$$

Further, we note that the lower bound of the multiparticle concurrence for mixed states [given in Eq. (9)] can be expressed as a combination of purities evaluated on subsystems $A\subset\{1,\ldots,N\}$ of the N-party space, as

$$
C(\varrho) \geqslant 2^{1-N/2}\sqrt{1 - \sum_{A\subseteq\{1,\ldots,N\}}\mathrm{tr}(\varrho_A^2) + (4-2^{2-N})\mathrm{tr}(\varrho^2)}.
\tag{A7}
$$

Hence, using Eq. (A6) together with the well-known formula for the purity in terms of randomized measurements [30], i.e.,

$$
\mathrm{tr}(\varrho^2) = d^N\sum_{\boldsymbol{s},\boldsymbol{s}'}(-d)^{-D(\boldsymbol{s},\boldsymbol{s}')}\overline{P_U(\boldsymbol{s})P_U(\boldsymbol{s}')},
\tag{A8}
$$

where $D(\boldsymbol{s},\boldsymbol{s}')$ denotes the Hamming distance [as explained after Eq. (11)], we directly arrive at the expression (11) for the lower bound (A7) in terms of randomized population probabilities

$$
\begin{aligned}
&C_N(\varrho)^2 \\
&\geqslant 2^{2-N} - 2^{2(1-N)}\sum_{A\subseteq\{1,\ldots,N\}}\mathrm{tr}(\varrho_A^2) + (4-2^{2-N})\mathrm{tr}(\varrho^2) \\
&= 2^{2-N} - 2^{2(1-N)}d^N(d+1)^N\sum_{\boldsymbol{s}\in\{0,1\}^N}\mathbb{E}_U[P_U(\boldsymbol{s})^2] \\
&\quad + (4-2^{2-N})d^N\sum_{\boldsymbol{s},\boldsymbol{s}'}(-d)^{D(\boldsymbol{s},\boldsymbol{s}')}\mathbb{E}_U[P_U(\boldsymbol{s})P_U(\boldsymbol{s}')].
\end{aligned}
\tag{A9}
$$

2. Multiparticle concurrence as a function of the moments (4)

We further note that Eqs. (A6) and (A9) can alternatively be expressed as a function of the moments (4), introduced in Sec. II A. To do so, we remind the reader of the representation of N-particle quantum states in terms of its sector lengths, along the lines of Refs. [37,52]. First, we note that a state ϱ can always be expressed as

$$
\varrho = \frac{1}{d^N}\sum_{i_1,\ldots,i_N=0}^{d^2-1}c_{i_1,\ldots,i_N}\lambda_{i_1}\otimes\cdots\otimes\lambda_{i_N},
\tag{A10}
$$

where λ_0 is the identity and λ_i are the Gell-Mann matrices, normalized such that $\lambda_i = \lambda_i^\dagger$, $\mathrm{tr}(\lambda_i\lambda_j) = d\delta_{ij}$, and $\mathrm{tr}(\lambda_i) = 0$ for $i > 0$. The real coefficients $c_{i_1\cdots i_N}$ are given by $c_{i_1\cdots i_N} = \mathrm{tr}(\varrho\lambda_{i_1}\otimes\cdots\otimes\lambda_{i_N}) = \langle\lambda_{i_1}\otimes\cdots\otimes\lambda_{i_N}\rangle$. The state ϱ can be represented by

$$
\varrho = \frac{1}{d^N}(\mathbb{1}^{\otimes n} + \hat{A}_1 + \hat{A}_2 + \cdots + \hat{A}_N),
\tag{A11}
$$

where the Hermitian operators $\hat{A}_k$, with $k = 1,\ldots,N$, denote the sum of all terms coming from the basis elements with weight k,

$$
\hat{A}_k(\varrho) = \sum_{\substack{i_1,\ldots,i_N=0,\\ \mathsf{w}(\lambda_{i_1}\otimes\cdots\otimes\lambda_{i_N})=k}}^{d^2-1}c_{i_1\cdots i_N}\lambda_{i_1}\otimes\cdots\otimes\lambda_{i_N},
\tag{A12}
$$

where the weight $\mathsf{w}(\lambda_{i_1}\otimes\cdots\otimes\lambda_{i_N})$ is equal to the number of nonidentity Gell-Mann matrices in the product $\lambda_{i_1}\otimes\cdots\otimes\lambda_{i_N}$. Now we can define sector lengths as

$$
A_k(\varrho) = \frac{1}{d^n}\mathrm{tr}[\hat{A}_k(\varrho)^2] = \sum_{\substack{i_1,\ldots,i_N=0,\\ \mathsf{w}(\lambda_{i_1}\otimes\cdots\otimes\lambda_{i_N})=k}}^{d^2-1}c_{i_1\cdots i_N}^2.
\tag{A13}
$$

Physically, the sector lengths A_k quantify the amount of k-body quantum correlations. Note that $A_0 = \alpha_{0\cdots 0} = 1$ due to $\mathrm{tr}(\varrho) = 1$. The sector lengths A_k can be associated with the purity of ϱ:

$$
\mathrm{tr}(\varrho^2) = \frac{1}{d^N}\sum_{i_1,\ldots,i_N=0}^{d^2-1}c_{i_1\cdots i_N}^2 = \frac{1}{d^N}\sum_{k=0}^{N}A_k(\varrho).
\tag{A14}
$$

Further, as shown in Refs. [21,37], the sector lengths (A14) are directly related to the moments (4) evaluated on the respective qudit sectors

$$
\frac{1}{(d^2-1)^k}A_k(\varrho) = \sum_{|A|=k}\mathcal{R}_A^{(2)}(\varrho),
\tag{A15}
$$

where $A = \{i_1,\ldots,i_k\}\subset\{1,\ldots,N\}$ with cardinality k. Hence, using Eq. (A14), the purity can be expressed as a sum of the second-order moments evaluated on all possible subsets A, as

$$
\begin{aligned}
\mathrm{tr}(\varrho^2) &= \frac{1}{d^N}\sum_{k=0}^{N}(d^2-1)^k\sum_{|A|=k}\mathcal{R}_A^{(2)}(\varrho) \\
&= \frac{1}{d^N}\sum_{A\subset\{1,\ldots,N\}}(d^2-1)^{|A|}\mathcal{R}_A^{(2)}(\varrho).
\end{aligned}
\tag{A16}
$$

Finally, it is straightforward to express the pure-state concurrence (6) as a function of second-order moments by invoking Eq. (A16):

$$
\begin{aligned}
C_N(|\psi\rangle) &= 2\sqrt{1 - \sum_{A\subset\{1,\dots,N\}} \sum_{A'\subset A} \frac{(d^2-1)^{|A'|}}{2^N d^{|A|}} \mathcal{R}_{A'}^{(2)}} \\
&= 2\sqrt{\left(1 - \frac{1}{2^N}\right) - \sum_{A\subsetneq\{1,\dots,N\}} \sum_{A'\subset A} \frac{(d^2-1)^{|A'|}}{2^N d^{|A|}} \mathcal{R}_{A'}^{(2)}}.
\end{aligned}
$$

(A17)

Note that in Eq. (A17) we used that for pure states the purity of the total state is one which eliminates several summands, in particular, also those which are of cardinality $|A| = N$.

Evaluating Eq. (A17) for the special cases $N = 2, 3$ and $d = 2$ leads to

$$
\begin{aligned}
C_2(|\psi\rangle) &= \sqrt{1 - \frac{3}{2}\left(\mathcal{R}_1^{(2)} + \mathcal{R}_2^{(2)}\right)}, \\
C_3(|\psi\rangle) &= \frac{1}{\sqrt{2}}\left(\frac{15}{4} - 3\left(\mathcal{R}_1^{(2)} + \mathcal{R}_2^{(2)} + \mathcal{R}_3^{(2)}\right)\right. \\
&\quad \left. - \frac{3^2}{4}\left(\mathcal{R}_{12}^{(2)} + \mathcal{R}_{23}^{(2)} + \mathcal{R}_{13}^{(2)}\right)\right)^{1/2}.
\end{aligned}
$$

(A18)

Furthermore, for mixed states, we can analogously use Eq. (A16) to derive an expression of the lower bound (9) in terms of second moments only, yielding

$$
\begin{aligned}
C_N(\varrho)^2 &= 2 - 2^{2-N} \\
&\quad \times \sum_{A\subset\{1,\dots,N\}} \left(\frac{1}{2^{|A|}} \sum_{A'\subset A} 3^{|A'|} \mathcal{R}_{A'}^{(2)} + \frac{2}{2^N} 3^{|A|} \mathcal{R}_A^{(2)}\right).
\end{aligned}
$$

(A19)

APPENDIX B: EVALUATION OF STATISTICAL UNCERTAINTIES

1. Unbiased estimators and their variance

In an experiment one can estimate the population probabilities $P_U(s)$ (in the following we will sometimes drop the subscript U unless it is required by the context) only from a finite number K of projective measurements. Then the corresponding statistical estimator is given by $\tilde{P}(s) = Y(s)/K$, where $Y(s)$ is the absolute frequency with which the bit string s appears. Hence, the random variable $Y(s)$ is distributed according to a multinomial distribution with probabilities $\{P(s)\}_{s\in\{0,1\}^N}$ and K trials. Exploiting this fact, one can find unbiased estimators $\tilde{P}^{(k)}(s)$ for the kth power of the population probability $P(s)^k$ by making the ansatz $\tilde{P}^{(k)}(s) = \sum_{i=0}^{k} \alpha_i [\tilde{Y}(s)/K]^i$ with the condition that $\mathbb{E}_{\text{multi}}[\tilde{P}^{(k)}(s)] = P(s)^k$. For the three lowest orders this results in

$$
\tilde{P}^{(2)}(s) = \frac{\tilde{P}(s)[K\tilde{P}(s) - 1]}{K - 1} = \tilde{P}(s)\frac{K\tilde{P}(s) - 1}{K - 1},
$$

(B1)

$$
\begin{aligned}
\tilde{P}^{(3)}(s) &= \frac{\tilde{P}(s)[K\tilde{P}(s) - 1][K\tilde{P}(s) - 2]}{(K-1)(K-2)} \\
&= \tilde{P}^{(2)}(s)\frac{K\tilde{P}(s) - 2}{K - 2},
\end{aligned}
$$

(B2)

$$
\begin{aligned}
\tilde{P}^{(4)}(s) &= \frac{\tilde{P}(s)[K\tilde{P}(s) - 1][K\tilde{P}(s) - 2][K\tilde{P}(s) - 3]}{(K-1)(K-2)(K-3)} \\
&= \tilde{P}^{(3)}(s)\frac{K\tilde{P}(s) - 3}{K - 3},
\end{aligned}
$$

(B3)

and similarly for products of population probabilities $P(s)P(s')$, with $s \neq s'$, we obtain

$$
\tilde{P}^{(1,1)}(s, s') = \frac{Y(s)Y(s')}{K(K-1)} = \frac{K}{K-1}\tilde{P}(s)\tilde{P}(s').
$$

(B4)

Moreover, also the expectation value $\mathbb{E}_U[\cdots]$ taken with respect to the local measurement settings can only be estimated based on finite samples of measurement bases, which finally leads to the definition of the unbiased estimators reported in Eqs. (18) and (19).

Further, we have to investigate the variance of the estimators (18) and (19) in order to get a handle on their associated statistical error. We start with the calculation of the variance of Eq. (18), which reads

$$
\begin{aligned}
\text{Var}[\overline{P_U^2(s)}] &= \frac{1}{M^2} \sum_{i=1}^{M} \text{Var}[\tilde{P}_{U_i}^{(2)}(s)] \\
&= \frac{1}{M} \mathbb{E}_{U,\text{multi}}\left[\left[\tilde{P}_{U_i}^{(2)}(s)\right]^2\right] - \mathbb{E}_U[P(s)^2]^2,
\end{aligned}
$$

(B5)

where we used that individual samples of local unitary transformations U_i are independent and identically distributed. In order to further evaluate the expression (B5) we have to exploit the moments of the multinomial distribution

$$
\begin{aligned}
\mathbb{E}_{\text{multi}}[\tilde{P}^{(2)}(s)] &= \frac{1}{K^2}\mathbb{E}_{\text{multi}}[Y(s)^2] \\
&= \frac{1}{K}[(K-1)P(s)^2 - P(s)],
\end{aligned}
$$

(B6)

$$
\begin{aligned}
\mathbb{E}_{\text{multi}}[\tilde{P}^{(3)}(s)] &= \frac{1}{K^2}[(K-1)(K-2)P(s)^3 \\
&\quad + 3(K-1)P(s)^2 + P(s)],
\end{aligned}
$$

(B7)

$$
\begin{aligned}
\mathbb{E}_{\text{multi}}[\tilde{P}^{(4)}(s)] &= \frac{1}{K^3}[(K-1)(K-2)(K-3)P(s)^4 \\
&\quad + 6(K-1)(K-2)P(s)^3 \\
&\quad + 7(K-1)P(s)^2 + P(s)],
\end{aligned}
$$

(B8)

leading to

$$
\begin{aligned}
&\mathbb{E}_{U,\text{multi}}[[\tilde{P}^{(2)}(s)]^2] \\
&= \mathbb{E}_{U,\text{multi}}\left[\frac{K^2\tilde{P}(s)^4 - 2K\tilde{P}(s)^3 + \tilde{P}(s)^2}{(K-1)^2}\right] \quad \text{(B9)} \\
&= \frac{\mathbb{E}_U[K^2\mathbb{E}_{\text{multi}}[\tilde{P}(s)^4] - 2K\mathbb{E}_{\text{multi}}[\tilde{P}(s)^3] + \mathbb{E}_{\text{multi}}[\tilde{P}(s)^2]]}{(K-1)^2} \\
&= \frac{\mathbb{E}_U[(K-2)(K-3)P(s)^4 + 4(K-2)P(s)^3 + 2P(s)^2]}{K(K-1)}.
\end{aligned}
$$

(B10)

Now we can write the variance as

$$
\begin{aligned}
\mathrm{Var}\big[\overline{P_U^2(s)}\big] &= \frac{1}{MK(K-1)}\big\{(K-2)(K-3)\mathbb{E}_U\big[P_U^4(s)\big] \\
&\quad + 4(K-2)\mathbb{E}_U\big[P_U^3(s)\big] + 2\mathbb{E}_U\big[P_U^2(s)\big]\big\} \\
&\quad - \frac{\mathbb{E}_U\big[P_U^2(s)\big]^2}{M}.
\end{aligned}
\tag{B11}
$$

An analogous calculation can be applied in the case of the estimator (19), leading to the expression for its variance

$$
\begin{aligned}
&\mathrm{Var}[\overline{P_U(s)P_U(s')}] \\
&= \frac{1}{MK(K-1)}\big((K-2)(K-3)\mathbb{E}_U\big[P_U^2(s)P_U^2(s')\big] \\
&\quad + (K-2)\big\{\mathbb{E}_U\big[P_U^2(s)P_U(s')\big] + \mathbb{E}_U\big[P_U(s)P_U^2(s')\big]\big\} \\
&\quad + \mathbb{E}_U[P_U(s)P_U(s')]\big) - \frac{1}{M}\mathbb{E}_U[P_U(s)P_U(s')]^2.
\end{aligned}
\tag{B12}
$$

We note that all the (cross) moments contained in Eqs. (B11) and (B12) can be evaluated using the expression

$$
\mathbb{E}_U\big[P_U^t(s)P_U^k(s')\big] = D_{d,t}^N \mathrm{tr}\!\left(\varrho^{\otimes t}\bigotimes_{i=1}^N \begin{Bmatrix} P_+^{(i)}, & s_i = s_i' \\ A_{t,k}^{(i)}, & s_i \neq s_i' \end{Bmatrix}\right),
\tag{B13}
$$

where $P_+^{(i)}$ denotes the projector onto the symmetric subspace [see Eq. (A4)] acting on the ith particle and $A_{t,k}^{(i)}$ is defined as

$$
A_{t,k}^{(i)} = \mathbb{E}_{u_i}\big[u_i^{\otimes(t+k)}|0\rangle\langle 0|^{\otimes t}\otimes|1\rangle\langle 1|^{\otimes k}(u_i^\dagger)^{\otimes(t+k)}\big].
\tag{B14}
$$

Note that from Eq. (B13) it becomes clear that the variance (B12) depends on the Hamming distance between the bit strings s and s'.

In conclusion, we see that the information about the statistical error of the estimators (18) and (19) is encoded in the (cross) moments (B13). In the following we will evaluate these quantities exactly for a set of typical multiparticle states, i.e., the N-qubit ground state, the GHZ state, and the Haar random states, and derive symbolic expressions that hold for an arbitrary number of particles N.

2. Variance of typical multiparticle states

a. Product state

For a random N-qubit product state we have $\varrho^{\otimes t} = \bigotimes_{i=1}^N |\varphi_i\rangle\langle\varphi_i|^{\otimes t}$, leading directly to the expressions

$$
\begin{aligned}
\mathbb{E}_U\big[P_U^t(s)\big] &= D_{d,t}^N \mathrm{tr}\!\left(\bigotimes_{i=1}^N |\varphi_i\rangle\langle\varphi_i|^{\otimes t}\bigotimes_{i=1}^N P_+^{(i)}\right) \\
&= D_{d,t}^N \prod_{i=1}^N \mathrm{tr}(|\varphi_i\rangle\langle\varphi_i|^{\otimes t}P_+^{(i)}) \\
&= D_{d,t}^N \mathrm{tr}(|0\rangle\langle 0|^{\otimes t}P_+)^N,
\end{aligned}
\tag{B15}
$$

which can be evaluated easily using Eq. (27).

b. GHZ state

For the N-qubit GHZ state we have

$$
\varrho = \frac{1}{2}\sum_{i,i'}(\delta_{i,0}\delta_{i',0} + \delta_{i,0}\delta_{i',1} + \delta_{i,1}\delta_{i',0} + \delta_{i,1}\delta_{i',1})|i\rangle\langle i'|,
\tag{B16}
$$

which can be directly used to analytically evaluate the expectation value of the higher-order population probabilities

$$
\begin{aligned}
\mathbb{E}_U\big[P_U^t(s)\big] &= \frac{D_{d,t}^N}{2^t}\big\{([P_+]_{0,\dots,0,0,\dots,0})^N + ([P_+]_{0,\dots,1,0,\dots,0})^N \\
&\quad + \cdots + ([P_+]_{1,\dots,1,1,\dots,1})^N\big\}.
\end{aligned}
\tag{B17}
$$

where $[P_+]_{i,i'}$ denotes the respective matrix element (i, i') of the projector P_+. Analogously, we find for the cross terms

$$
\begin{aligned}
&\mathbb{E}_U[P_U^t(s)P_U^k(s')] \\
&= \frac{D_{d,t}^N}{2^t}\big\{([P_+]_{0,\dots,0,0,\dots,0})^{N-D(s,s')}([A^{t,k}]_{0,\dots,0,0,\dots,0})^{D(s,s')} \\
&\quad + ([P_+]_{0,\dots,1,0,\dots,0})^{N-D(s,s')}([A^{t,k}]_{0,\dots,1,0,\dots,0})^{D(s,s')} + \cdots \\
&\quad + ([P_+]_{1,\dots,1,1,\dots,1})^{N-D(s,s')}([A^{t,k}]_{1,\dots,1,1,\dots,1})^{D(s,s')}\big\}.
\end{aligned}
\tag{B18}
$$

c. Haar random states

Finally, for Haar random states we evaluate the expected average variance as

$$
\begin{aligned}
\mathbb{E}\big[\mathrm{Var}\big[\overline{P_U^2(s)}\big]\big] &= \frac{1}{MK(K-1)}\big\{(K-2)(K-3)\mathbb{E}_{\psi,U}\big[P_U^4(s)\big] \\
&\quad + 4(K-2)\mathbb{E}_{\psi,U}\big[P_U^3(s)\big] + 2\mathbb{E}_{\psi,U}\big[P_U^2(s)\big]\big\} \\
&\quad - \frac{1}{M}\mathbb{E}\big[\mathbb{E}_U\big[P_U^2(s)\big]^2\big],
\end{aligned}
\tag{B19}
$$

which can be evaluated straightforwardly using Eq. (27). As $\mathbb{E}_U[P_U^2(s)]$ does not depend on the specific bit string under consideration, to improve the statistics in a real experiment one can also average over all different bit strings that were observed, i.e., $I = \{s_1, \dots, s_{|I|}\} \subset \{0, 1\}^N$, by considering the estimator introduced in Eq. (20). Here, in general $|I| \leqslant K$ as maximally K different bit strings can be measured during K projective measurements. As for N qubits the maximal number of different possible bit strings is given by 2^N, we will estimate the number of different bit strings that occurred by $|I| = \min(2^N, K)$, which is a rough estimate justified for the specific choice of Haar random states. Having this in mind, we consider the variance of the estimator (20), yielding

$$
\begin{aligned}
\mathrm{Var}\big[\overline{P_U^2}\big] &= \frac{1}{M^2}\sum_{i=1}^M \frac{1}{|I|^2}\sum_{s,s'}\mathrm{Cov}\big[\tilde{P}_U^2(s), \tilde{P}_U^2(s')\big] \\
&= \frac{1}{M^2}\sum_{i=1}^M \frac{1}{|I|^2}\bigg(\sum_s \mathrm{Var}\big\{\big[\tilde{P}_U^2(s)\big]_i\big\} \\
&\quad + \sum_{s\neq s'}\mathrm{Cov}\big[\big(\tilde{P}_U^2(s), \tilde{P}_U^2(s')\big)_i\big]\bigg).
\end{aligned}
\tag{B20}
$$

In general, the term $\mathrm{Cov}[\tilde{P}_U^2(s), \tilde{P}_U^2(s')]$ is difficult to evaluate analytically. However, for Haar random states the correlations

between the probabilities of different outcomes s and s' are exponentially small in the number of qubits [64,65]. Therefore,

in the case of Haar random states and large system sizes it is well justified to approximate the variance as

$$\mathrm{Var}\left(\overline{P_U^2}\right) \approx \frac{1}{M}\frac{1}{|I|}\mathrm{Var}\left[\overline{P_U^2(s)}\right]. \tag{B21}$$

Similarly for the product term, we can also determine the expected variance

$$\mathbb{E}_\psi[\mathrm{Var}[\overline{P_U(s)P_U(s')}]] = \frac{1}{MK(K-1)}((K-2)(K-3)\mathbb{E}_{\psi,U}\left[P_U^2(s)P_U^2(s')\right] + (K-2)\{\mathbb{E}_{\psi,U}\left[P_U^2(s)P_U(s')\right] + \mathbb{E}_{\psi,U}\left[P_U(s)P_U^2(s')\right]\}$$

$$+ \mathbb{E}_{\psi,U}[P_U(s)P_U(s')]) - \frac{1}{M}\mathbb{E}_\psi[\mathbb{E}_U[P_U(s)P_U(s')]^2]. \tag{B22}$$

Here $\mathbb{E}_{\psi,U}[P_U^n(s)P_U^m(s')]$ can be evaluated once again using Eq. (27). However, note that $\mathbb{E}_\psi[\mathrm{Var}[\overline{P_U(s)P_U(s')}]]$ depends explicitly on the specific bit strings s and s'.

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, New York, 2000).

[2] H. Buhrman, R. Cleve, S. Massar, and R. de Wolf, Rev. Mod. Phys. **82**, 665 (2010).

[3] F. Arute *et al.*, Nature (London) **574**, 505 (2019).

[4] M. Kjaergaard, M. E. Schwartz, J. Braumüller, P. Krantz, J. I.-J. Wang, S. Gustavsson, and W. D. Oliver, Annu. Rev. Condens. Matter Phys. **11**, 369 (2020).

[5] F. Graselli, G. Murta, J. de Jong, F. Hahn, D. Bruß, H. Kampermann, and A. Pappa, PRX Quantum **3**, 040306 (2022).

[6] Z. Ren, W. Li, A. Smerzi, and M. Gessner, Phys. Rev. Lett. **126**, 080502 (2021).

[7] M. Van den Nest, Phys. Rev. Lett. **110**, 060504 (2013).

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

[9] O. Gühne and G. Tóth, Phys. Rep. **474**, 1 (2009).

[10] J. Eisert, D. Hangleiter, N. Walk, I. Roth, D. Markham, R. Parekh, U. Chabaud, and E. Kashefi, Nat. Rev. Phys. **2**, 382 (2020).

[11] R. Blume-Kohout, New J. Phys. **12**, 043034 (2010).

[12] I. Šupić and J. Bowles, Quantum **4**, 337 (2020).

[13] M. Gluza, M. Kliesch, J. Eisert, and L. Aolita, Phys. Rev. Lett. **120**, 190501 (2018).

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

[15] C. A. Riofrío, D. Gross, S. T. Flammia, T. Monz, D. Nigg, R. Blatt, and J. Eisert, Nat. Commun. **8**, 15305 (2017).

[16] J. Carrasquilla, G. Torlai, R. G. Melko, and L. Aolita, Nat. Mach. Intell. **1**, 155 (2019).

[17] Y.-C. Liang, N. Harrigan, S. D. Bartlett, and T. Rudolph, Phys. Rev. Lett. **104**, 050401 (2010).

[18] S. T. Flammia and Y.-K. Liu, Phys. Rev. Lett. **106**, 230501 (2011).

[19] P. Shadbolt, T. Vértesi, Y.-C. Liang, C. Branciard, N. Brunner, and J. L. O'Brien, Sci. Rep. **2**, 470 (2012).

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

[21] M. C. Tran, B. Dakić, F. Arnault, W. Laskowski, and T. Paterek, Phys. Rev. A **92**, 050301(R) (2015).

[22] M. C. Tran, B. Dakić, W. Laskowski, and T. Paterek, Phys. Rev. A **94**, 042302 (2016).

[23] M. Walschaers, J. Kuipers, J.-D. Urbina, K. Mayer, M. C. Tichy, K. Richter, and A. Buchleitner, New J. Phys. **18**, 032001 (2016).

[24] T. Giordani *et al.*, Nat. Photon. **12**, 173 (2018).

[25] A. Ketterer, N. Wyderka, and O. Gühne, Phys. Rev. Lett. **122**, 120505 (2019).

[26] A. Ketterer, N. Wyderka, and O. Gühne, Quantum **4**, 325 (2020).

[27] M. Krebsbach, M.Sc. thesis, Albert-Ludwigs-Universität Freiburg, 2019, available at https://freidok.uni-freiburg.de/data/150706.

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

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

[30] T. Brydges, A. Elben, P. Jurcevic, B. Vermersch, C. Maier, B. P. Lanyon, P. Zoller, R. Blatt, and C. F. Roos, Science **364**, 260 (2019).

[31] A. Elben, B. Vermersch, C. F. Roos, and P. Zoller, Phys. Rev. A **99**, 052323 (2019).

[32] V. Saggio, A. Dimić, C. Greganti, L. A. Rozema, P. Walther, and B. Dakić, Nat. Phys. **15**, 935 (2019).

[33] L. Knips, J. Dziewior, W. Kłobus, W. Laskowski, T. Paterek, P. J. Shadbolt, H. Weinfurter, and J. D. A. Meinecke, npj Quantum Inf. **6**, 51 (2020).

[34] A. Elben, B. Vermersch, R. van Bijnen, C. Kokail, T. Brydges, C. Maier, M. K. Joshi, R. Blatt, C. F. Roos, and P. Zoller, Phys. Rev. Lett. **124**, 010504 (2020).

[35] A. Elben, R. Kueng, H.-Y. R. Huang, R. van Bijnen, C. Kokail, M. Dalmonte, P. Calabrese, B. Kraus, J. Preskill, P. Zoller, and B. Vermersch, Phys. Rev. Lett. **125**, 200501 (2020).

[36] S.-X. Yang, G. N. Tabia, P.-S. Lin, and Y.-C. Liang, Phys. Rev. A **102**, 022419 (2020).

[37] S. Imai, N. Wyderka, A. Ketterer, and O. Gühne, Phys. Rev. Lett. **126**, 150501 (2021).

[38] A. Ketterer, S. Imai, N. Wyderka, and O. Gühne, Phys. Rev. A **106**, L010402 (2022).

[39] L. Knips, Quantum Views **4**, 47 (2020).

[40] N. Wyderka and A. Ketterer, arXiv:2211.09610.

[41] S. Liu, Q. He, M. Huber, O. Gühne, and G. Vitagliano, arXiv:2211.09614.

[42] N. Wyderka, A. Ketterer, S. Imai, J. L. Bönsel, D. E. Jones, B. T. Kirby, X.-D. Yu, and O. Gühne, arXiv:2212.07894.

[43] S. Aaronson, *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing* (ACM, New York, 2018).

[44] H.-Y. Huang, R. Kueng, and J. Preskill, Nat. Phys. **16**, 1050 (2020).

[45] M. Paini, A. Kalev, D. Padilha, and B. Ruck, Quantum **5**, 413 (2021).

[46] F. Mintert, M. Kuś, and A. Buchleitner, Phys. Rev. Lett. **92**, 167902 (2004).

[47] A. R. R. Carvalho, F. Mintert, and A. Buchleitner, Phys. Rev. Lett. **93**, 230501 (2004).

[48] F. Mintert, A. R. R. Carvalho, M. Kuś, and A. Buchleitner, Phys. Rep. **415**, 207 (2005).

[49] L. Aolita and F. Mintert, Phys. Rev. Lett. **97**, 050501 (2006).

[50] F. Mintert and A. Buchleitner, Phys. Rev. Lett. **98**, 140505 (2007).

[51] L. Aolita, A. Buchleitner, and F. Mintert, Phys. Rev. A **78**, 022308 (2008).

[52] N. Wyderka and O. Gühne, J. Phys. A: Math. Theor. **53**, 345302 (2020).

[53] S. Ohnemus, M.Sc. thesis, Albert-Ludwigs-Universität Freiburg, 2021, available at https://doi.org/10.6094/UNIFR/227071.

[54] Z. Liu, P. Zeng, Y. Zhou, and M. Gu, Phys. Rev. A **105**, 022407 (2022).

[55] A. Borras, A. P. Majtey, A. R. Plastino, M. Casas, and A. Plastino, Phys. Rev. A **79**, 022112 (2009).

[56] C. Dankert, M.Sc. thesis, University of Waterloo, 2005.

[57] P. D. Seymour and T. Zaslavsky, Adv. Math. **52**, 213 (1984).

[58] F. G. S. L. Brandão, A. W. Harrow, and M. Horodecki, Phys. Rev. Lett. **116**, 170502 (2016).

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

[60] J. Haferkamp, F. Montealegre-Mora, M. Heinrich, J. Eisert, D. Gross, and I. Roth, Commun. Math. Phys. **397**, 995 (2023).

[61] Z. Webb, Quantum Inf. Comput. **16**, 1379 (2016).

[62] H. Zhu, R. Kueng, M. Grassl, and D. Gross, arXiv:1609.08172.

[63] K. D. Schmidt, *Maß und Wahrscheinlichkeit* (Springer, Heidelberg, 2011).

[64] N. Ullah, Nucl. Phys. **58**, 65 (1964).

[65] D. Petz and J. Réffy, Period. Math. Hung. **49**, 103 (2004).

[66] B. Collins and P. Sniady, Commun. Math. Phys. **264**, 773 (2006).

[67] D. Weingarten, J. Math. Phys. **19**, 999 (1978).

[68] M. Ledoux, *The Concentration of Measure Phenomenon* (American Mathematical Society, Providence, 2001).

[69] M. Tiersch, F. de Melo, and A. Buchleitner, J. Phys. A: Math. Theor. **46**, 085301 (2013).

[70] R. Jozsa and A. Miyake, Proc. R. Soc. A **464**, 3089 (2008).

[71] D. J. Brod and A. M. Childs, Quantum Inf. Comput. **14**, 901 (2014).

[72] B. M. Terhal and D. P. DiVincenzo, Phys. Rev. A **65**, 032325 (2002).

[73] D. Shepherd and M. J. Bremner, Proc. R. Soc. A **465**, 1413 (2009).

[74] M. J. Bremner, R. Josza, and D. Shepherd, Proc. R. Soc. A **467**, 459 (2011).

[75] Y. Nakata and M. Murao, Eur. Phys. J. Plus **129**, 152 (2014).

[76] R. O. Vallejos, F. de Melo, and G. G. Carlo, Phys. Rev. A **104**, 012602 (2021).

[77] K. Fujii and T. Morimae, New J. Phys. **19**, 033003 (2017).