

ARTICLE OPEN

Single-copy entanglement detection

Aleksandra Dimić¹ and Borivoje Dakić^{1,2,3}

One of the main challenges of quantum information is the reliable verification of quantum entanglement. The conventional detection schemes require repeated measurement on a large number of identically prepared systems. This is hard to achieve in practice when dealing with large-scale entangled quantum systems. In this letter we formulate verification as a decision procedure, i.e., entanglement is seen as the ability of quantum system to answer certain “yes-no questions”. We show that for a variety of large quantum states even a single copy suffices to detect entanglement with a high probability by using local measurements. For example, a single copy of a 16-qubit k -producible state or one copy of 24-qubit linear cluster state suffices to verify entanglement with more than 95% confidence. Our method is applicable to many important classes of states, such as cluster states or ground states of local Hamiltonians in general.

npj Quantum Information (2018)4:11 ; doi:10.1038/s41534-017-0055-x

INTRODUCTION

A main focus of modern practical quantum information research is on the generation of large-scale quantum entanglement involving many particles with the goal of achieving real applications of quantum technologies.^{1,2} Recent quantum experiments dealing with a large number of particles, such as optical lattice simulations involving 10^3 – 10^4 atoms,^{3–6} experiments with hundreds of trapped ions⁷ or thousands of qubits in D-Wave systems (See: <https://www.dwavesys.com/>), show the real potential for applications of quantum technologies in the near future. An important instance of this challenge is the verification problem, i.e., how to reliably detect the presence of quantum resources, in particular quantum entanglement. The plausibility of standard verification schemes is questionable, since they require repeated measurement on large ensemble of identically prepared copies, which is highly demanding to achieve in practice.

One way of detecting quantum entanglement is to perform full quantum state tomography⁸ from which one can extract full information about the quantum state preparation (one can recover the entire density matrix). However, the full tomography becomes an unrealistic task already for a moderate size of quantum systems as the number of required measurement settings grows exponentially fast with the size of system. Luckily, in many cases, the knowledge of the entire quantum state is not needed, i.e., one can witness the presence of entanglement by measuring the mean values or the higher moments of a moderate number of physical quantities (observables). This is the groundwork for detection methods based on witness operators,^{9–14} non-linear entanglement witnesses,^{15–17} Bell’s inequalities,^{18,19} quantum Fisher information^{20–23} and random correlations.^{24–26} These methods have been proven extremely useful for many practical situations and they have been extensively developed for the detection of a variety of quantum states and adapted to various scenarios (see review articles^{27–29}). Nevertheless, all of the existing detection schemes are based on an idealized situation which

requires repeated measurements on a large ensemble of independent and identically distributed (i.i.d.) copies of a quantum state.

The typical detection procedure involves the extraction of the mean value of a certain witness operator $W = \sum_i W_i$, by measuring the means of the local observables $W_i = A_1 \otimes \dots \otimes A_N$ (N is the size of system). Therefore, in order to detect entanglement, one has to conduct different experiments (different measurement settings for each W_i), each of which requires a large number of identically prepared copies such that the sample averages are close to the real mean values. However, as any practical situation deals with a finite amount of data generated by a quantum measurement, the presence of entanglement can be verified only with a certain level of confidence, thus an adequate statistical analysis is necessary.^{30–32} Moreover, it is very hard to fulfil these requirements when dealing with large-scale entangled systems as only a limited (rather low) number of instances of a given quantum resource is available, due to various technical challenges, such as the lack of a good control and manipulation. As an example, one can take a recent experiment done with single photons³³ where a 10-photon coincidence was registered every 5 min in average. With the same technology, that is by using the parametric down-conversion and postselection techniques, every additional photon pair (e.g., 12, 14, ... photons) would reduce the count rate by at least one order of magnitude, consequently making the duration of the experiment (to verify entanglement) months or even years longer. In such situations, where only a limited number of resources is available, the main question arises whether it is still possible to reliably and efficiently certify the presence of quantum entanglement? This question is not only interesting from the theoretical point of view, it is also of great importance for practical quantum information.

In recent years we have seen several works that go beyond i.i.d. scenario, in the context of quantum state tomography³⁴ and reliable entanglement verification.^{17,32} Although the techniques

¹Faculty of Physics, University of Belgrade, Studentski Trg 12-16, 11000 Belgrade, Serbia; ²Institute for Quantum Optics and Quantum Information (IQOQI), Austrian Academy of Sciences, Boltzmanngasse 3, A-1090 Vienna, Austria and ³Vienna Center for Quantum Science and Technology (VCQ), Faculty of Physics, University of Vienna, Boltzmanngasse 5, Vienna A-1090, Austria

Correspondence: Borivoje Dakić (borivoje.dakic@univie.ac.at)

Received: 31 August 2017 Revised: 7 December 2017 Accepted: 11 December 2017
Published online: 15 February 2018

and methods developed there are quite generic, they still require a large sample sizes to verify entanglement with high confidence. On the other hand, in situations where only a low number of instances of a given quantum resource are available it appears natural to employ random sampling techniques³⁵ for reliable detection. The advantage of such methods comes from simplicity of the data analysis, since minimal prior knowledge of the global population is needed. In the quantum scenario, random sampling has been proven very useful for quantum communication complexity,^{36,37} tomography via compressed sensing,³⁸ fidelity estimation,³⁹ self-testing methods,^{40–45} quantum state certification,^{46,47} quantum secret sharing,⁴⁸ and verification of quantum computing.⁴⁹ Some of these methods can be used to verify entanglement probabilistically as demonstrated in^{50,51}. In the same spirit, we shall incorporate random sampling methods together with techniques of quantum communication complexity^{36,37} to propose entanglement verification scheme in the form of a quantum information task. Unlike focusing on a large ensemble of i.i.d. copies, our main target here is a single experimental run, i.e., the central quantity for entanglement detection is the probability of success to perform certain binary task, given that the state was entangled/separable. Therefore, our scheme is designed to detect entanglement probabilistically. This framework has two main advantages as compared to conventional detection schemes:

- it promises a dramatic reduction of the resources needed for reliable verification in large quantum systems, and
- it provides a simple tool for reliable statistical analysis of errors and confidence intervals.

Most importantly, we show that in many situations the probability of success (to accomplish certain binary task) decreases exponentially fast with the size of system for all separable input states, whereas it approaches certainty if a particular entangled state (the target state) was prepared. Thus, even a single experimental run (single copy) can reveal the presence of entanglement with high accuracy. To our best knowledge, this is the first demonstration of entanglement detection in a single-copy regime (apart from the well-studied example of an i.i.d. state $\rho^{\otimes N}$, see example of k -producible state below). We explicitly construct the detection procedure for k -producible states⁵² and cluster states.⁵³ We show that, for example, one copy of a 16-qubit k -producible state or a single-copy of 24-qubit linear cluster state suffices to certify entanglement with more than 95% confidence. Thus, our method is applicable for quantum experiments involving tens of entangled qubits with the promise of a dramatic reduction of the resources needed for reliable entanglement detection (as compared to standard methods). Furthermore, the method developed for k -producible states can be used to naturally embed the standard techniques based on entanglement witnesses into our framework, meaning the statistical analysis of confidence intervals and errors simple and straightforward. Finally, we develop a general method for entanglement detection in ground states of local Hamiltonians (that exhibit the so-called entanglement gap¹³). These include many important classes of quantum states, such as the matrix product states⁵⁴ and projected-entangled pair states⁵⁵ as they can be seen as unique ground states of the so-called parent Hamiltonians.^{54,56} At the end, we analyze the noise effect and we show that our probabilistic detection is very robust against the noise modeled by an arbitrary separable state.

RESULTS

Detection framework

Our method relies on a decision procedure where entanglement is seen as the ability of quantum systems to answer certain “yes-no

questions”. The main figure of merit is the probability of success that a certain binary cost function F evaluates to 1, i.e., $P[F=1]$. The main goal is to provide examples of quantum states where P decreases exponentially fast to zero as the size of system grows for all separable states, whereas it approaches certainty ($P=1$) if a particular entangled state (the target state) was prepared. Therefore, one can verify the presence of quantum entanglement with high probability even by measuring a single copy of a large quantum system.

In order to explain how our scheme works we consider a quantum system composed of N subsystems each residing in a finite-dimensional Hilbert space of dimension d . We usually assume N is large, although all the formulas derived hold for general N . To each subsystem we associate a certain set of possible measurements that can be performed locally. For example, in the case of qubits we may chose to measure each of them in complementary bases (such as X and Z measurement). In the general case, we shall include the most general quantum measurements (POVMs). Thus to each subsystem we associate a set of M different measurement settings defined by the set of positive semidefinite operators $E_{mi}^{(k)}$, where $\sum_i E_{mi}^{(k)} = 1$ and $m = 1 \dots M$. Here k labels the subsystem, m the measurement setting and i labels the measurement outcome.

Given a single-copy of an N -partite quantum system, the detection procedure consists of the following four steps (see Fig. 1):

1. A sequence of measurement settings $\{m_1, m_2, \dots, m_N\}$ is randomly generated from the probability distribution of settings $\Pi(m_1, \dots, m_N)$,
2. The measurements are locally executed on each subsystem and the set of outcomes $\{i_1, \dots, i_N\}$ is obtained,
3. A certain binary (0/1) cost function of settings and outcomes $F_{[N]} = F_{m_1 \dots m_N}^{i_1 \dots i_N}$ is computed,
4. If $F_{[N]} = 0/1$ we associate “success/failure” to the experimental run.

This is the way to establish the probabilistic framework for entanglement detection through the probability of success $P[F_{[N]} = 1]$. Our goal here is to choose the cost functions such that the probability of success vanishes exponentially fast in N for all

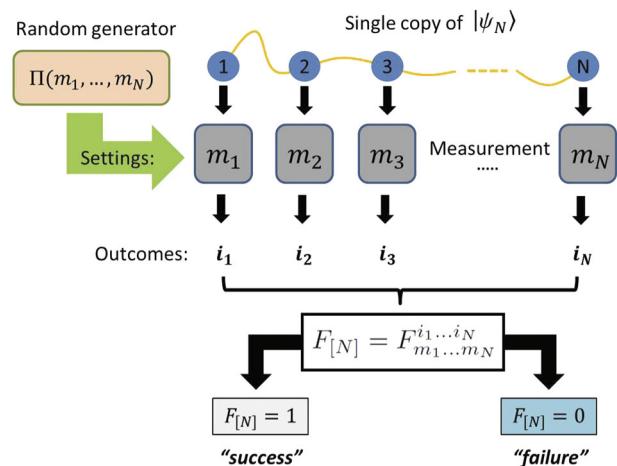


Fig. 1 Probabilistic entanglement detection. A single-copy of N -partite quantum state is prepared. The sequence of measurement settings $\{m_1, \dots, m_N\}$ is randomly drawn from distribution $\Pi(m_1, \dots, m_N)$. Each m_k is locally executed on k th subsystem and the set of outcomes $\{i_1, \dots, i_N\}$ is obtained. The value of binary cost function $F_{[N]} = F_{m_1 \dots m_N}^{i_1 \dots i_N}$ prescribes either “success” ($F_{[N]} = 1$) or “failure” ($F_{[N]} = 0$) to the experimental run

separable states ρ_{sep}

$$P_{\rho_{\text{sep}}} [F_{[N]} = 1] \leq \exp[-Nc], \quad (1)$$

where $c > 0$ is some constant. On the other hand, the cost function $F_{[N]}$ is chosen such that there is an entangled state for which $P_{\rho_{\text{ent}}} [F_{[N]} = 1] \approx 1$, meaning that whenever the state ρ_{ent} (target state) has been prepared, the detection scheme works even in a single-copy scenario. An explicit bound on the probability of success for concrete examples will be derived.

Example of k -producible state

A good example to start with is that of the k -producible entangled state,⁵² i.e., $|\phi_1\rangle|\phi_2\rangle\dots|\phi_m\rangle$, where the products $|\phi_s\rangle$ involve at most k parties. For simplicity, we chose the target state to be the product of quantum singlets $|\psi_0\rangle = |\psi^-\rangle^{\otimes N}$, where $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ (The example and task presented here is quiet similar to “non-local” quantum games (see refs. 36,37)). Nevertheless, we believe it is a good starting point for introducing a more delicate examples that follow in subsequent sections). We consider the set of $\{X, Y, Z\}$ measurement settings for each qubit, meaning that the measurement is performed in the eigenbasis of Pauli operators with the set of binary outcomes $i=0, 1$. The quantum singlet is the unique state for which $X \otimes X = Y \otimes Y = Z \otimes Z = -1$, meaning that the measurement of $X \otimes X$, $Y \otimes Y$, and $Z \otimes Z$ reveals perfect anticorrelations. Let us introduce the projectors on the outcome -1 for the correlation measurement

$$Q = \frac{1 - X \otimes X}{2} \quad (2)$$

$$W = \frac{1 - Y \otimes Y}{2} \quad (3)$$

$$R = \frac{1 - Z \otimes Z}{2}. \quad (4)$$

To these projectors we associate three measurement settings $S = \{XX, YY, ZZ\}$. Although, the projectors are commutative, there is no separable state for which the measurement reveals $Q = W = R = 1$ simultaneously (this is a property of the singlet state only). Therefore, if we pick one of the settings from S randomly (with probability 1/3), there is a chance of at most 2/3 to get the outcome 1 for all separable inputs. More precisely, in such a case, the probability of success

$$P_{\rho_{\text{sep}}} = \left\langle \frac{1}{3}(Q + W + R) \right\rangle \leq \frac{2}{3}, \quad (5)$$

for all separable two-qubit states ρ_{sep} . Here $\langle \cdot \rangle = \text{Tr}(\cdot)\rho$ denotes the mean value. This observation clearly suggests a detection scheme. We shall divide the set of $2N$ qubits into consecutive pairs and for every individual pair we pick one of the settings from S randomly (with probability 1/3) and perform the corresponding correlation measurement (2), (3) and (4). For separable inputs, the bound (5) suggests that the relative frequency of the outcome 1 cannot significantly exceed the value of 2/3 (provided that N is large). Formally, we define the frequency $R_{[N]} = \sum_{k=1}^N F_k$, where F_k is the outcome of the correlation measurement on individual pairs

$$F_k = \frac{1}{2} \left(1 - (-1)^{i_k j_k} \right). \quad (6)$$

Here $i_k j_k = 0, 1$ label the single-qubit measurement outcomes for the k th pair. The cost function is defined as

$$F_{[N]} = \begin{cases} 1, & R_{[N]} \geq \left(\frac{2}{3} + \delta\right)N; \\ 0, & R_{[N]} < \left(\frac{2}{3} + \delta\right)N, \end{cases} \quad (7)$$

where $\delta > 0$ is some constant we keep at the moment as a free parameter. In other words, we associate “success” to the run if the number of local successes F_k exceeds certain threshold of

$\left(\frac{2}{3} + \delta\right)N$. The overall probability of success reads

$$P_{\rho} [F_{[N]} = 1] = P_{\rho} \left[F_1 + \dots + F_N \geq \left(\frac{2}{3} + \delta\right)N \right], \quad (8)$$

and we recognize in the last equation the probability that the sum of random variables $F_1 + \dots + F_N$ exceeds the value of $\left(\frac{2}{3} + \delta\right)N$. If the input state is a product state $\rho_{\text{prod}} = \rho_1 \otimes \dots \otimes \rho_{2N}$, the random variables F_k are independent with $\langle F_k \rangle \leq \frac{2}{3}$. For such a case the bound on (8) is well studied in classical probability theory and the results are known as the Chernoff bounds.⁵⁷ We show in the Appendix that

$$P_{\rho_{\text{prod}}} [F_{[N]} = 1] \leq e^{-D\left(\frac{2}{3} + \delta\right)\frac{2}{3}N}, \quad (9)$$

where $D(x||y) = x \log \frac{x}{y} + (1-x) \log \frac{1-x}{1-y} \geq 0$ is the Kullback–Leibler divergence. Furthermore, if the bound holds for all product states, it also holds for their mixtures, i.e., it holds for all separable states. We see that the probability of success vanishes exponentially fast in N , for all $\delta > 0$. This is quite convenient, as we do not have to fix δ in advance. Once the experiment has been performed, we can calculate directly from the experimental data F_1, F_2, \dots, F_N how much the frequency deviates from $2N/3$, i.e., we set $\delta = (F_1 + \dots + F_N)/N - 2/3$, and consequently calculate the bound on probability of success for separable states by using (9). For the case of $|\psi_0\rangle = |\psi^-\rangle^{\otimes N}$ input state, each local cost function $F_k = 1$ deterministically, thus we get $\delta = 1/3$. The bound (9) reduces to

$$P_{\rho_{\text{sep}}} [F_{[N]} = 1] \leq \left(\frac{2}{3}\right)^N. \quad (10)$$

If N is sufficiently large, a single-copy of $|\psi_0\rangle$ suffices to certify presence of entanglement with high probability. For example, if we want to have a detection probability of at least 95% (i.e., we want to be sure that no separable state has a probability of success more than 5%) in a single-shot experiment, we get the minimal number $N_{\min} = 8$, which is a remarkably low number.

The present example shows how the standard detection of entanglement in quantum singlet based on the witness operator $\frac{1}{3}(Q + W + R)$ can be naturally embedded in our framework. Conventionally, one has to measure Q , W , and R in three separate experiments by using an i.i.d. ensemble of qubit pairs $\rho_{12}^{\otimes N}$ in order to estimate the mean values $\langle Q \rangle$, $\langle W \rangle$ and $\langle R \rangle$. However, the i.i.d. assumption is difficult to justify operationally, hence the statistical analysis involving many experiments is non-trivial. Furthermore, if the number of singlet pairs is low, it is not clear how to actually pursue the detection scheme. For example, imagine a situation where only $N = 8$ pairs are available. The question is how to divide the pairs and perform the corresponding measurements. We may use the first three copies to measure Q , the second three to measure W , and the last two for the measurement of R . However, if the order is known and fixed in advance, than the following product state $(|x+\rangle|x-\rangle)^{\otimes 3}(|y+\rangle|y-\rangle)^{\otimes 3}(|z+\rangle|z-\rangle)^{\otimes 2}$ gives exactly the same result as the i.i.d. state $|\psi^-\rangle^{\otimes 8}$. Thus, we cannot conclude the presence of entanglement or we may even wrongly claim its presence. Certainly, a correct statement requires a proper statistical analysis. On the other hand, one of the key procedures in our method is the random sampling of measurement settings, which provides us a simple tool to analyze the errors and confidence intervals through the probability of success. Therefore, there is a clear separation between the state $|\psi^-\rangle^{\otimes 8}$ and the product state given above, as the later has only the chance of $(2/3)^8 \approx 0.039$ to reveal the result $F_1 + \dots + F_8 = 8$.

In general, any detection based on witness operator can be incorporated in our framework, with the goal to achieve more resource-efficient entanglement detection. For a witness $W = \sum_i W_i$, one has to sample the measurements of W_i 's randomly every single experimental run. The bound similar to (9) can be easily derived. Nevertheless, one may object that in

such a case, one still requires many copies for reliable detection (i.e., N copies of k -partite state $|\psi\rangle$ folded into a single multipartite copy $|\psi\rangle^{\otimes N}$). In the next examples we will unambiguously show that, indeed, one can certify entanglement by measuring only a single-copy.

Example of cluster states

Another example we present here is that of cluster states.⁵³ In contrast to the previous example of k -producible states, cluster states contain genuine multipartite entanglement⁵⁸ and they are known to be a universal resource for measurement-based quantum computation.⁵³ For the sake of simplicity, we shall explain how the single-copy detection scheme works for the case of linear cluster states (LCS). The generalization to higher dimensions is straightforward and we briefly discuss it at the end of this section. The N -qubit LCS is uniquely defined by the set of 2^N stabilizers, i.e.,

$$G_{q_1 \dots q_N} |LCS\rangle = G_1^{q_1} \dots G_N^{q_N} |LCS\rangle = +1 |LCS\rangle, \quad (11)$$

where $G_k = Z_{k-1} X_k Z_{k+1}$ and $q_k = 0, 1$. Here $\{X_k, Y_k, Z_k\}$ represent the set of standard Pauli matrices acting on k th qubit and, for simplicity, we have chosen the cluster state with periodic boundaries, i.e., $Z_{N+1} \stackrel{\text{def}}{=} Z_1$ and $X_{N+1} \stackrel{\text{def}}{=} X_1$. We consider the set of $\{X, Y, Z\}$ measurement settings for each qubit, meaning that the measurement is performed in the eigenbasis of Pauli operators with the set of binary outcomes $i=0,1$. We start with a simple analysis by considering a small subset (cluster) of four qubits, let say $\{1, 2, 3, 4\}$ with the corresponding stabilizers $G_2 = Z_1 X_2 Z_3$, $G_3 = Z_2 X_3 Z_4$ and $G_2 G_3 = Z_1 Y_2 Y_3 Z_4$ acting solely on it. Although, all three stabilizers are commutative, they are not locally compatible (in a sense that there is no local measurement of all three of them simultaneously), therefore there is no product (separable) state for which all three observables can take the same value, i.e., $G_2 = G_3 = G_2 G_3 = +1$, simultaneously. For that reason, if we randomly chose (with probability 1/3) to measure one of the stabilizers there is only a chance of 2/3 to get the result +1, for all separable inputs (similar to the previous example of singlet state). This is the key observation that enables our detection method to work. Our main idea is to show that if we pick a random partition of the set of N qubits into 4-qubit clusters and subsequently on each of them randomly measure one of the corresponding stabilizers, the relative frequency of the outcome +1 cannot significantly exceed the value of 2/3. More formally, we start by introducing partitions of N qubits into 4-qubit clusters $\{c_{t_1}, c_{t_2}, \dots, c_{t_L}\}$, where c_{t_s} is the cluster involving the sequence of four qubits $c_{t_s} = \{t_s, t_s + 1, t_s + 2, t_s + 3\}$. Furthermore, we see from the previous analysis that the border qubits in each cluster are always measured in the Z -basis (when measuring the corresponding stabilizer). Thus, we shall allow for possible overlap between neighbouring clusters on border qubits. More precisely, we say that the partition is regular if the neighbouring clusters overlap on at most one (border) qubit, i.e., $t_{s+1} - t_s \geq 3$. For example, the partition $\{\dots, \{7, 8, 9, 10\}, \{10, 11, 12, 13\}, \dots\}$ is considered regular, whereas $\{\dots, \{7, 8, 9, 10\}, \{9, 10, 11, 12\}, \dots\}$ is irregular, as the two clusters in partition overlap on qubits 9 and 10 (see SI for more examples). We denote the set of all regular partitions of size L by \mathcal{C}_L . We shall think of L as being large, e.g., on the same scale as $O(N)$ with the number of qubits and, at the same time, we shall choose L such that the set \mathcal{C}_L is large in size as well. The clusters in the partition serve as the building-blocks for the construction of the cost function $F_{[N]}$. For every cluster c_{t_s} in the partition there are three stabilizers associated to it: $G_{t_s+1} = Z_{t_s} X_{t_s+1} Z_{t_s+2}$, $G_{t_s+2} = Z_{t_s+1} X_{t_s+2} Z_{t_s+3}$ and $G_{t_s+1, t_s+2} = G_{t_s+1} G_{t_s+2} = Z_{t_s} Y_{t_s+1} Y_{t_s+2} Z_{t_s+3}$. To

each of them we associate three projectors

$$Q_{t_s} = \frac{1 + G_{t_s+1}}{2}, \quad (12)$$

$$W_{t_s} = \frac{1 + G_{t_s+2}}{2}, \quad (13)$$

$$R_{t_s} = \frac{1 + G_{t_s+1} G_{t_s+2}}{2}, \quad (14)$$

that project on the +1 outcome. We associate the following measurement settings with each projector

$$\{ZXZZ, ZZXZ, ZYYZ\}, \quad (15)$$

and we assign “success” to the cluster measurement only if the outcome +1 (for the value of measured stabilizer) occurs. Formally speaking, for every cluster we define the following local cost function

$$F_s = F_m^{i_1 i_2 i_3 i_4} = \frac{1}{2} + \frac{1}{2} \begin{cases} (-1)^{i_1 + i_2 + i_3}, & m = ZXZZ; \\ (-1)^{i_2 + i_3 + i_4}, & m = ZZXZ; \\ (-1)^{i_1 + i_2 + i_3 + i_4}, & m = ZYYZ, \end{cases} \quad (16)$$

where $s = 1 \dots L$. Finally, for a given partition $\{c_{t_1}, c_{t_2}, \dots, c_{t_L}\}$ the overall cost function is defined in the following way

$$F_{[N]} = \begin{cases} 1, & F_1 + \dots + F_L \geq (\frac{2}{3} + \delta)L; \\ 0, & F_1 + \dots + F_L < (\frac{2}{3} + \delta)L, \end{cases} \quad (17)$$

where $\delta > 0$ is some constant we keep at the moment as a free parameter. In other words, we associate the “success” to the run if the number of local successes exceeds a certain threshold of $(\frac{2}{3} + \delta)L$. We have defined all we need to set-up the detection procedure. Firstly, a particular partition $\{c_{t_1}, c_{t_2}, \dots, c_{t_L}\}$ is randomly generated from the set \mathcal{C}_L (with probability $1/|\mathcal{C}_L|$). Secondly, for each cluster in the partition we pick randomly (with probability 1/3) one setting from the set (15) and execute the corresponding measurement. The experimental run reveals the sequence of results F_1, F_2, \dots, F_L from which we evaluate $F_{[N]}$ by using (17).

Now, we will show that the probability of success vanishes exponentially fast for all separable states as the number of qubits grows. Firstly, for a fixed partition $\{c_{t_1}, c_{t_2}, \dots, c_{t_L}\}$ it is clear that product states fail to satisfy $F_s = 1$ for all three settings $\{ZXZZ, ZZXZ, ZYYZ\}$, because XZ, ZX, YY are locally incompatible on a second and third cluster qubit. Thus, if the settings are uniformly distributed (with probability of 1/3), one can easily show that the probability of success for individual clusters

$$P_{\rho_{\text{prod}}} [F_s = 1] = \langle F_s \rangle = \frac{1}{3} \langle Q_{t_s} + W_{t_s} + R_{t_s} \rangle \leq \frac{2}{3}, \quad (18)$$

for all product states $\rho_{\text{prod}} = \rho_1 \otimes \dots \otimes \rho_N$. Furthermore, if the input state is a product state, the local cost functions F_s can be seen as independent binary (0/1) random variables with $\langle F_s \rangle \leq 2/3$ for all $s = 1 \dots L$. The overall probability of success reads

$$P_{\rho_{\text{prod}}} [F_{[N]} = 1] = P_{\rho_{\text{prod}}} \left[F_1 + \dots + F_L \geq \left(\frac{2}{3} + \delta \right) L \right], \quad (19)$$

and we recognize in the last equation the probability that the sum of independent random variables $F_1 + \dots + F_L$ exceeds the value of $(\frac{2}{3} + \delta)L$. As $\langle F_s \rangle \leq 2/3$ we expect that the sum $F_1 + \dots + F_L$ cannot exceed $2/3L$ significantly. Similar to the previous example (of singlet state), the Chernoff bound holds (see Appendix for the proof), i.e.,

$$P_{\rho_{\text{prod}}} [F_{[N]} = 1] \leq e^{-D(\frac{2}{3} + \delta || \frac{2}{3})L}, \quad (20)$$

where $D(x||y)$ is the Kullback–Leibler divergence. Furthermore, if the bound holds for all product states, it also holds for their mixtures, i.e., it holds for all separable states. Thus, as long as L

grows with N (for example we can set $L = \lceil N/5 \rceil$, where $\lceil \cdot \rceil$ denotes the integer part) the probability of success vanishes exponentially fast, for all $\delta > 0$. As before, we do not have to fix δ in advance. Once the experiment has been performed, we can calculate directly from the experimental data F_1, F_2, \dots how much the sum of results deviates from $2L/3$, i.e., we set $\delta = (F_1 + \dots + F_L)/L - 2/3$, and consequently calculate the bound on probability of success for separable states by using (20). For the case of cluster state preparation $|LCS\rangle$, each local cost function $F_s = 1$ deterministically, thus we get $\delta = 1/3$. The bound (20) reduces to

$$P_{\rho_{\text{sep}}} [F_{[N]} = 1] \leq \left(\frac{2}{3}\right)^L. \quad (21)$$

If the number of qubits is sufficiently large, even a single-copy of LCS suffices to certify presence of entanglement with high probability. For example, if we want to have a detection probability of at least 95% (i.e., we want to be sure that no separable state has a probability of success more than 5%) in a single-shot experiment, we get the minimal number of clusters $L_{\min} = 8$. The lowest number of qubits with such support is $N = 24$. Nevertheless, in such a case the set of all partitions \mathcal{C}_L reduces to three only, and for the reason explained below (see discussion at the end of this section), one may want to have $|\mathcal{C}_L|$ significantly larger. For example, already $N = 25$ has $|\mathcal{C}_L| = 25$, for $N = 26$ we get $|\mathcal{C}_L| = 117$ etc. The scheme can be used not only to detect entanglement, it can be also used to certify the presence of LCS. To see this, note that $P_\rho [F_{[N]} = 1] = \text{Tr } \rho \Pi$, where

$$\Pi = \frac{1}{|\mathcal{C}_L|} \sum_{\{c_{t_1}, \dots, c_{t_L}\} \in \mathcal{C}_L} \prod_{s=1}^L \frac{1}{3} (Q_{t_s} + W_{t_s} + R_{t_s}). \quad (22)$$

Clearly LCS is the eigenstate $\Pi|LCS\rangle = 1|LCS\rangle$ for the maximal eigenvalue. Now, the operator Π can be expanded in terms of stabilizers $G_{q_1 \dots q_N}$ defined by the Eq. (11). If the set \mathcal{C}_L is sufficiently large the expansion will include all 2^N stabilizers. Since the LCS is the only state with $G_{q_1 \dots q_N}|LCS\rangle = +1|LCS\rangle$ for all stabilizers, we conclude that LCS is a unique eigenstate of Π for eigenvalue 1. Thus, the LCS state is the only state with the maximal probability of success, i.e., $P[F_{[N]} = 1] = 1$.

We shall briefly comment on the type of entanglement certified by the single-copy detection scheme. Firstly, if we are willing to detect multipartite entanglement, it is very important that the set \mathcal{C}_L is large in size. Recall, that the bound (20) holds for arbitrary partition from the set \mathcal{C}_L for all separable states. Therefore, if the partition $\{c_{t_1}, \dots, c_{t_L}\}$ is fixed and known in advance, the bound (20) still holds. Nevertheless, for such a case, the following 4-producible state $|\phi\rangle = |\psi_1\rangle|\psi_2\rangle \dots |\psi_L\rangle$, where $|\psi\rangle_s$ is the common eigenstate for all three projectors Q_{t_s}, W_{t_s} and R_{t_s} (for eigenvalue 1), reveals $F_s = 1$ deterministically for every cluster. Consequently we have $P[F_{[N]} = 1] = 1$ for $|\phi\rangle$ being the input state. Such a state contains localized entanglement on individual clusters (blocks of entanglement). To prevent $|\phi\rangle$ maximizing the probability of success, a random choice of partition from a large set \mathcal{C}_L is necessary. For example, already including additional partition $\{c_{t_1+1}, \dots, c_{t_L+1}\}$ obtained by shifting one qubit to the right, prevents $|\phi\rangle$ to be the common eigenstate of $Q_{t_s}, W_{t_s}, R_{t_s}$ and $Q_{t_s+1}, W_{t_s+1}, R_{t_s+1}$. On the other hand, if we want $F_{[N]} = 1$ deterministically for both partitions, entanglement between neighbouring clusters is needed. Thus, if all partitions of large \mathcal{C}_L are included, the only way to have non-trivial probability of success is to input delocalized entanglement.

Finally, let us briefly explain the generalization to the higher dimensional case. Take an example of a 2D cluster state (known to be universal for quantum computation). Here, one can introduce partitions into 4×4 qubit clusters with the corresponding stabilizer projectors (in analogy to Q_{t_s}, W_{t_s} and R_{t_s} for LCS) and define the local cost functions. In complete analogy to the 1D

case, the 2D detection scheme consists of drawing a random partition followed by a random measurement of local projectors on individual clusters. The separable bound similar to (20) can be derived. On the other hand, if the 2D cluster state has been prepared, the probability of success is 1.

Ground states of local Hamiltonians

One of the reasons that single-copy entanglement detection works for cluster states can be associated to the robustness of entanglement with respect to local perturbations. For example, if we measure one or even a group of localized qubits in cluster state, entanglement remains present between the rest qubits. Ground states of local Hamiltonians are believed to share this property (robustness of entanglement),⁵⁹ therefore we can expect that they are also amendable to single-copy verification. Here we show that indeed this is the case.

Consider a L -local Hamiltonian on some graph of N particles $H = \sum_{k=1}^N H^{(k)}$, where $H^{(k)}$ acts on at most L subsystems (L is fixed and independent of N). For simplicity reason, we assume the number of local terms $H^{(k)}$ to match the number of particles N (this is common for many physical situations, see for example⁶⁰). One may consider a more general case where the number of local terms grows as a polynomial function of N . Nevertheless, the detection scheme shall work the same way. Let $|\psi_0\rangle$ is the ground state $H|\psi_0\rangle = N\epsilon_0|\psi_0\rangle$, where $\epsilon_0 = N\epsilon_0$ is the ground-state energy. We are interested in Hamiltonians that exhibit the so-called entanglement gap $g_E = \epsilon_s - \epsilon_0 > 0$,¹³ where $\epsilon_s = \frac{1}{N} \min_{\rho_{\text{sep}}} \text{Tr } H \rho_{\text{sep}}$ is the minimal achievable energy (per particle) by a separable state. Furthermore, we assume g_E to be finite and non-zero in the thermodynamical limit, i.e., $0 < \lim_{N \rightarrow \infty} g_E < +\infty$. To summarize, we are interested in Hamiltonians where the mean energy $\langle H \rangle$ can serve as the entanglement witness, i.e., $\langle H \rangle \geq N\epsilon_s$ for all separable states, whereas at least the ground state violates this bound.

We shall develop a general scheme that works for arbitrary local Hamiltonian. For that reason we introduce a set of tomographically complete measurements for each particle. For example, in the case of qubits, a natural choice are the three complementary measurements defined by X , Y , and Z Pauli operators. Thus, the set of measurement operators $E_{mi}^{(k)}$ forms a complete basis in the space of observables, i.e., any observable $A^{(k)}$ acting on k th subsystem can be decomposed as $A^{(k)} = \sum_{mi} a_{mi} E_{mi}^{(k)}$. Here $m = 1 \dots M$ and $i = 1 \dots D$, where M is the number of settings and D is the number of outcomes. Furthermore, in order to simplify the notation, we introduce a new variable $x_k = (m_k, i_k)$ which labels a pair of measurement setting and outcome, hence $E_{x_k}^{(k)}$ refers to $E_{m_k i_k}^{(k)}$. Note that $\sum_{x_k} E_{x_k}^{(k)} = M1^{(k)}$.

For a given local Hamiltonian $H = \sum_{k=1}^N H^{(k)}$, operator $H^{(k)}$ acts on at most L neighbouring subsystems (neighbours of k including k itself). It is convenient to introduce the $N \times L$ “neighbouring” matrix $n_{k,l}$, where $n_{k,1}, \dots, n_{k,L}$ is a sequence of integers labeling all the neighbours of k th subsystem (including k th subsystem itself) on which the local operator $H^{(k)}$ acts. The “neighbouring” matrix can be seen as the list of neighbourhoods $(\mathcal{N}(1), \dots, \mathcal{N}(N))$, where $\mathcal{N}(k)$ denotes the set of all neighbours of k . For example, the notation $\{n_{3,1}, n_{3,2}, n_{3,3}\} = \{2, 3, 4\}$ means that $H^{(3)}$ acts on subsystems 2, 3 and 4. Because the set of measurement operators is tomographically complete, each $H^{(k)}$ can be decomposed into the sum of products of local measurement operators

$$H^{(k)} = \sum_{x_1 \dots x_L} h_{x_1 \dots x_L}^{(k)} E_{x_1}^{(n_{k,1})} \dots E_{x_L}^{(n_{k,L})}. \quad (23)$$

The operator $H^{(k)}$ can be completely identified with the tensor $h^{(k)} = h_{x_1 \dots x_L}^{(k)}$. Similarly, the full Hamiltonian H reads

$$H = \sum_{x_1 \dots x_N} H_{x_1 \dots x_N} E_{x_1}^{(1)} \dots E_{x_N}^{(N)}, \quad (24)$$

where we set $M^{N-L} H_{x_1 \dots x_N} = \sum_{k=1}^N h_{x_{n_{k,1}} \dots x_{n_{k,L}}}^{(k)}$ (the factor M^{N-L}

comes because of the normalization $\sum_x E_x = M1$. Now we can set-up the detection procedure. Firstly, we pick measurement settings for individual subsystems randomly (i.e., with probability $1/M$) and generate the sequence $\{m_1, \dots, m_N\}$. The measurements are executed on local subsystems and the set of outcomes $\{i_1, \dots, i_N\}$ is obtained. Equivalently, we say that the sequence of random variables $\{x_1, \dots, x_N\}$ is generated, where $x_k = (m_k, i_k)$. Now, we shall define the cost function $F_{[N]}$. It is convenient to define $H_{[N]} = M^N H_{x_1 \dots x_N} = M^L \sum_{k=1}^N h^{(k)}$. A straightforward inspection shows $\langle H_{[N]} \rangle = \text{Tr} \rho H = \langle H \rangle$, thus the classical random variable $H_{[N]}$ can serve to extract the mean value of Hamiltonian $\langle H \rangle$. Since $\langle H \rangle \geq N\epsilon_s$ holds for all separable states, it is natural to choose the following cost function

$$F_{[N]} = \begin{cases} 1, & H_{[N]} \leq N(\epsilon_s - \delta); \\ 0, & H_{[N]} > N(\epsilon_s - \delta), \end{cases} \quad (25)$$

where $0 < \delta < \epsilon_s - \epsilon_0 = g_E$ is constant we keep at the moment as a free parameter. Since the random variable $H_{[N]}$ completely captures properties of Hamiltonian, we expect $H_{[N]}$ not to precede the separable bound $N\epsilon_s$ significantly in a single-shot experiment (provided that N is large). Indeed, in the Appendix we show that for all separable states ρ_{sep} the following bound holds

$$P_{\rho_{\text{sep}}} [F_{[N]} = 1] \leq \exp[-Nk^2\delta^2], \quad (26)$$

where $\kappa > 0$ is constant. Thus, the probability of success vanishes exponentially fast with N for all separable inputs. On the other hand, if the ground state $|\psi_0\rangle$ is prepared, we show in the Appendix that the probability of success reaches 1 in the thermodynamical limit, i.e.,

$$P_{\psi_0} [F_{[N]} = 1] \geq 1 - \frac{\beta^2}{N(g_E - \delta)^2}, \quad (27)$$

where $\beta > 0$ is constant. In other words, if N is sufficiently large, the probability of success is close to 1.

There are several points worth of mentioning here. Firstly, the previous example of cluster states can be incorporated in the present scheme, since cluster states can be seen as unique ground-states of local Hamiltonians.⁶¹ Nevertheless, the detection scheme introduced in the previous section is more resource-efficient for cluster states for the following reasons: a) the bound (20) is more tight than (26), and b) the probability of success evaluates to 1 (for the cluster-state input), in contrast to (27) which reaches 1 asymptotically. On the other hand, the ground-state detection method has certain practical advantages. Namely, one of the crucial elements for detection is the use of tomographically complete set of measurements. In principle, they can be substituted by a single informationally complete POVM (ICPOVM).⁶² More precisely, instead of a set of tomographically complete measurements, a single POVM with the measurement operators E_i forming a complete basis in the space of observables, can be used. Thus, an N -partite Hamiltonian can be expressed as $H = \sum_{i_1 \dots i_N=1}^D h_{i_1 \dots i_N} E_{i_1}^{(1)} \dots E_{i_N}^{(N)}$, where $i_k = 1 \dots D$ labels the measurement outcome. The properties of Hamiltonian are fully captured by the classical random variable $H_{[N]} = h_{i_1 \dots i_N}$ (function of the measurement outcomes i_1, \dots, i_N). Now, there is no random sampling of measurement settings, there is only one measurement (ICPOVM) for each particle. The variable $H_{[N]}$ is calculated from the set of measurement outcomes $\{i_1, \dots, i_N\}$. The cost function is defined as (25), and derivation of bounds (20) and (26) is essentially the same as before. Formally, both methods are equivalent. Nevertheless, practical advantage of using ICPOVM compared to random sampling of measurement settings can be significant in certain cases, conditioned on the physical implementation of POVM. For example, if ICPOVM is implemented by using additional degrees of freedom (e.g., for the case of single-photons by combining the path and polarization degree of freedom⁶³), then, the same, single measurement setting is applied

on every local subsystem. This is very convenient when dealing with large-scale quantum systems, for which full manipulation and addressability of individual particles is demanding to achieve.

Tolerance to noise

Here we analyze the effects of noise on probabilistic entanglement detection. Consider an N -partite target state ρ_0 with the probability of success $p_0 > 0$, i.e., there is a chance of p_0 to get success (detect entanglement) in a single experimental run (if the state ρ_0 has been prepared). This means that in practice, one needs in average $1/p_0$ copies of ρ_0 in order to detect entanglement (if the probability of success is p_0 than $1/p_0$ experimental runs are needed in average to get "success"). Furthermore, let the separable bound (1) hold, i.e., the probability of success is exponentially small in N for all separable inputs. Now, consider a mixture $\rho = \lambda \rho_{\text{sep}} + (1 - \lambda) \rho_0$, where ρ_{sep} is an arbitrary separable state and $0 < \lambda < 1$ quantifies the amount of noise. For example, in many cases the noise can be modeled via the white noise $\rho_{\text{sep}} = 1/d^N$ (here d is the dimension of local Hilbert space) or the product colored noise $\rho_{\text{sep}} = \rho_1 \otimes \dots \otimes \rho_N$.^{64,65} The probability of success for such a state is a mixture of probabilities, i.e., $P_{\rho} = \lambda P_{\rho_{\text{sep}}} + (1 - \lambda) P_{\rho_0} \approx (1 - \lambda) p_0$, as long as $(1 - \lambda) p_0$ is significantly larger than $P_{\rho_{\text{sep}}} = O(\exp[-Nc])$. This means that noise affects detection by suppressing the probability of success by the factor $1 - \lambda$, for any type of separable noise (i.e., modeled by a separable state). Therefore, one needs in average $\frac{1}{(1 - \lambda) p_0}$ experimental runs in order to verify the presence of entanglement. This a strong resistance to noise, as if $(1 - \lambda) p_0$ is not exponentially small in N (for example, we consider $(1 - \lambda) p_0 > 0$ constant and independent of N), entanglement can be verified with the constant cost in terms of resources (number of copies). On the other hand, the situation with standard detection methods is very different. Typically, a witness tolerates noise below a certain critical point, i.e., $\lambda < \lambda_c$. Thus, if noise passes the threshold, the scheme does not work even if an infinite number of resources is available.

To illustrate our findings, let us examine the example of a linear cluster state mixed with the white noise $\rho_{\text{LCS}} = \lambda 1/2^N + (1 - \lambda) |LCS\rangle\langle LCS|$, where $|LCS\rangle$ is the linear cluster state defined by the Eq. (11). The presence of entanglement can be detected via the following set of witness operators⁶⁶

$$W_k = 1 - G_k - G_{k+1}, \quad (28)$$

where the generators G_k are defined by the Eq. (11). One can easily show that $\langle W_k \rangle_{\text{sep}} \geq 0$ for all separable states. In contrast, for the linear cluster state preparation we have $\langle W_k \rangle_{\text{LCS}} = -1$, therefore the witness detects entanglement for $\lambda \leq 1/2$.⁶⁶ On the other hand, if our scheme is applied (see section "Example of cluster states"), the separable bound is given by the Eq. (20), where $\delta > 0$ is a free parameter. As before, we set $\delta = 1/3$ and we get the probability of success $P_{\text{sep}} \leq (\frac{2}{3})^L$ (see Eq. (21)), where L is the size of partitions. For N (and consequently L) being sufficiently large, $P_{\text{sep}} \approx 0$ is negligible. On the contrary, if the state ρ_{LCS} is prepared, the probability of success is lower bounded by $P_{\rho} = \lambda P_{1/2^N} + (1 - \lambda) P_{|LCS\rangle} \geq 1 - \lambda$, where we used $P_{|LCS\rangle} = 1$. This means that $1/(1 - \lambda)$ copies are sufficient in average in order to get success. For example, if we set $\lambda = 1/3$, we need three copies (in average) to detect entanglement, whereas in such a case, the witness (28) will fail to detect entanglement even if an infinite number of copies is supplied.

DISCUSSION

We introduced a probabilistic technique for resource-efficient entanglement detection in large-scale multiparticle quantum systems. We have shown that for variety of quantum states, probability to detect entanglement (as quantified by the

probability of success) approaches one exponentially fast with the size of system, implying that even a single copy suffices to verify entanglement with high probability. Our method promises a dramatic reduction of the resource needed for reliable entanglement verification, therefore it has great potential for practical applications in current and near future experiments aiming at generation and manipulation of massive entanglement.

ACKNOWLEDGEMENTS

The authors thank Nataša Dragović, Dragoljub Gočanin, Časlav Brukner, Lee Rozema and Philip Walther for helpful comments. A.D. acknowledges the support from the Serbian Ministry of Science (Project ON171035).

AUTHOR CONTRIBUTIONS

B.D. supervised the project, provided theoretical analysis and wrote the manuscript. A.D. provided theoretical analysis and wrote the manuscript.

ADDITIONAL INFORMATION

Supplementary information accompanies the paper on the *npj Quantum Information* website (<https://doi.org/10.1038/s41534-017-0055-x>).

Competing interests: The authors declare no competing financial interests.

Publisher's note: Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

REFERENCES

1. Castelvecchi, D. Quantum computers ready to leap out of the lab in 2017. *Nature* **541**, 9 (2017).
2. Dowling, J. P. & Milburn, G. J. Quantum technology: the second quantum revolution. *Philos. Trans. R. Soc. Lond. A: Math., Phys. Eng. Sci.* **361**, 1655 (2003).
3. Yan, B. et al. Realizing a lattice spin model with polar molecules. *Nature* **501**, 521 (2013). arXiv:1305.5598 [physics.atom-ph].
4. Hart, R. A. et al. Observation of anti-ferromagnetic correlations in the Hubbard model with ultra-cold atoms. *Nature* **519**, 211 (2015). arXiv:1407.5932 [cond-mat.quant-gas].
5. Takei, N. et al. Direct observation of ultrafast many-body electron dynamics in an ultra-cold Rydberg gas. *Nat. Commun.* **7**, 13449 (2016). arXiv:1504.03635 [physics.atom-ph].
6. Campbell, S. L. et al. A Fermi-degenerate three-dimensional optical lattice clock. ArXiv e-prints (2017). arXiv:1702.01210[physics.atomph].
7. Britton, J. W. et al. Engineered two-dimensional Ising interactions in a trapped-ion quantum simulator with hundreds of spins. *Nature* **484**, 489 (2012). arXiv:1204.5789 [quant-ph].
8. Bisio, A., Chiribella, G., D'Ariano, G. M., Facchini, S. & Perinotti, P. Optimal quantum tomography. *IEEE J. Sel. Top. Quant. Elect.* **15**, 1646 (2009).
9. Horodecki, M., Horodecki, P. & Horodecki, P. Separability of mixed states: necessary and sufficient conditions. *Phys. Letts. A* **223**, 1 (1996). quant-ph/9605038.
10. Terhal, B. M. Detecting quantum entanglement. *Theor. Comput. Sci.* **287**, 313 (2002).
11. Brukner, C. & Vedral, V. Macroscopic thermodynamical witnesses of quantum entanglement. eprint arXiv:quantph/0406040 (2004). quant-ph/0406040.
12. Tóth, G. Entanglement witnesses in spin models. *Phys. Rev. A* **71**, 010301 (2005).
13. Dowling, M. R., Doherty, A. C. & Bartlett, S. D. Energy as an entanglement witness for quantum manybody systems. *Phys. Rev. A* **70**, 062113 (2004).
14. Knips, L., Schwemmer, C., Klein, N., Wieśniak, M. & Weinfurter, H. Multipartite entanglement detection with minimal effort. *Phys. Rev. Lett.* **117**, 210504 (2016).
15. Gühne, O. & Lütkenhaus, N. J. Nonlinear entanglement witnesses, covariance matrices and the geometry of separable states. *Phys. Conf. Ser.* **67**, 012004 (2007). quant-ph/0612108.
16. Badziąg, P., Brukner, W., Laskowski, T., Paterek & Żukowski, M. Experimentally friendly geometrical criteria for entanglement. *Phys. Rev. Lett.* **100**, 140403 (2008).
17. Arrazola, J. M., Gittsovich, O. & Lütkenhaus, N. Accessible nonlinear entanglement witnesses. *Phys. Rev. A* **85**, 062327 (2012).
18. Wang, Z., Singh, S. & Navascués, M. Entanglement and nonlocality in infinite 1D systems. ArXiv e-prints (2016). arXiv:1608.03485[quant-ph].
19. Baccari, F., Cavalcanti, D., Wittek, P. & Acín, A. Efficient device-independent entanglement detection for multipartite systems. ArXiv e-prints (2016). arXiv:1612.08551[quant-ph].
20. Pezzé, L. & Smerzi, A. Entanglement, nonlinear dynamics, and the Heisenberg limit. *Phys. Rev. Lett.* **102**, 100401 (2009).
21. Hyllus, P. et al. Fisher information and multipartite entanglement. *Phys. Rev. A* **85**, 022321 (2012).
22. Tóth, G. Multipartite entanglement and high-precision measurements. *Phys. Rev. A* **85**, 022322 (2012).
23. Pezzè, L., Li, Y., Li, W. & Smerzi, A. Witnessing entanglement without entanglement witness operators. *Proc. Natl. Acad. Sci.* **113**, 11459 (2016). arXiv:1512.06213 [quant-ph].
24. Tran, M. C., Dakić, B., Arnault, F., Laskowski, W. & Paterek, T. Quantum entanglement from random measurements. *Phys. Rev. A* **92**, 050301 (2015).
25. Tran, M. C., Dakić, B., Laskowski, W. & Paterek, T. Correlations between outcomes of random measurements. *Phys. Rev. A* **94**, 042302 (2016).
26. Szangolies, J., Kampermann, H. & Bruß, D. Detecting entanglement of unknown quantum states with random measurements. *New. J. Phys.* **17**, 113051 (2015). arXiv:1504.08225 [quant-ph].
27. Gühne, O. & Tóth, G. Entanglement detection. *Phys. Rep.* **474**, 1 (2009).
28. Horodecki, R., Horodecki, P., Horodecki, M. & Horodecki, K. Quantum entanglement. *Rev. Mod. Phys.* **81**, 865 (2009).
29. Chruściński, D. & Sarbicki, G. Entanglement witnesses: construction analysis and classification. *J. Phys. A Math. Theor.* **47**, 483001 (2014).
30. Jungnitsch, B. et al. Increasing the statistical significance of entanglement detection in experiments. *Phys. Rev. Lett.* **104**, 210401 (2010).
31. Blume-Kohout, R., Yin, J. O. S. & van Enk, S. J. Entanglement verification with finite data. *Phys. Rev. Lett.* **105**, 170501 (2010).
32. Arrazola, J. M. et al. Reliable entanglement verification. *Phys. Rev. A* **87**, 062331 (2013).
33. Wang, X.-L. et al. Experimental ten-photon entanglement. *Phys. Rev. Lett.* **117**, 210502 (2016).
34. Christandl, M. & Renner, R. Reliable quantum state tomography. *Phys. Rev. Lett.* **109**, 120403 (2012).
35. Tillé, Y. in *International Encyclopedia of Statistical Science*, (ed. Lovric, M.) 1273–1274 (Springer, Berlin, Heidelberg, 2011).
36. Buhrman, H., Cleve, R., Massar, S. & de Wolf, R. Nonlocality and communication complexity. *Rev. Mod. Phys.* **82**, 665 (2010).
37. Brunner, N., Cavalcanti, D., Pironio, S., Scarani, V. & Wehner, S. Bell nonlocality. *Rev. Mod. Phys.* **86**, 419 (2014).
38. Gross, D., Liu, Y.-K., Flammia, S. T., Becker, S. & Eisert, J. Quantum state tomography via compressed sensing. *Phys. Rev. Lett.* **105**, 150401 (2010).
39. Flammia, S. T. & Liu, Y.-K. Direct fidelity estimation from few Pauli measurements. *Phys. Rev. Lett.* **106**, 230501 (2011).
40. Mayers, D. & Yao, A. Self testing quantum apparatus. eprint arXiv:quant-ph/0307205 (2003). quant-ph/0307205.
41. McKague, M. Self-testing graph states. ArXiv e-prints (2010). arXiv:1010.1989 [quant-ph].
42. Bancal, J.-D., Navascués, M., Scarani, V., Vértesi, T. & Yang, T. H. Physical characterization of quantum devices from nonlocal correlations. *Phys. Rev. A* **91**, 022115 (2015).
43. Miller, C. A. & Shi, Y. Optimal robust quantum self testing by binary nonlocal XOR games. ArXiv e-prints (2012). arXiv:1207.1819 [quant-ph].
44. Reichardt, B. W., Unger, F. & Vazirani, U. A classical leash for a quantum system: Command of quantum systems via rigidity of CHSH games. ArXiv e-prints (2012). arXiv:1209.0448 [quant-ph].
45. McKague, M., Yang, T. H. & Scarani, V. J. Robust self-testing of the singlet. *Phys. A: Math. Theor.* **45**, 455304 (2012).
46. Aolita, L., Gogolin, C., Kliesch, M. & Eisert, J. Reliable quantum certification of photonic state preparations. *Nat. Commun.* **6**, 8498 (2015). arXiv:1407.4817 [quantph].
47. Hangleiter, D., Kliesch, M., Schwarz, M. & Eisert, J. Direct certification of a class of quantum simulations. *Quantum Sci. Technol.* **2**, 015004 (2017).
48. Marin, A. & Markham, D. Practical sharing of quantum secrets over untrusted channels. ArXiv e-prints (2014). arXiv:1410.0556 [quant-ph].
49. Fitzsimons, J. F. & Kashe, E. Unconditionally verifiable blind quantum computation. *Phys. Rev. A* **96**, 012303 (2017).
50. Pappa, A., Chailloux, A., Wehner, S., Diamanti, E. & Kerenidis, I. Multipartite entanglement verification resistant against dishonest parties. *Phys. Rev. Lett.* **108**, 260502 (2012).
51. McCutcheon, W. et al. Experimental verification of multipartite entanglement in quantum networks. *Nat. Commun.* **7**, 13251 (2016). arXiv:1611.04772[quant-ph].
52. Gühne, O., Tóth, G. & Briegel, H. Multipartite entanglement in spin chains. *New. J. Phys.* **7**, 229 (2005).

53. Raussendorf, R. & Briegel, H. J. A one way quantum computer. *Phys. Rev. Lett.* **86**, 5188 (2001).

54. Perez-Garcia, D., Verstraete, F., Wolf, M. M. & Cirac, J. I. Matrix product state representations. *Quantum Inf. Comput.* **7**, 401 (2007). quant-ph/0608197.

55. Verstraete, F., Murg, V. & Cirac, J. I. Matrix product states, projected entangled pair states, and variational renormalization group methods for quantum spin systems. *Adv. Phys.* **57**, 143 (2008).

56. Perez-Garcia, D., Verstraete, F., Cirac, J. I. & Wolf, M. M. PEPS as unique ground states of local Hamiltonians. *Quantum Inf. Comput.* **8**, 0650 (2007). arXiv:0707.2260 [quant-ph].

57. Chernoff, H. *Ann. Math. Stat.* **23**, 493 (1952).

58. Hein, M., Eisert, J. & Briegel, H. J. Multiparty entanglement in graph states. *Phys. Rev. A* **69**, 062311 (2004).

59. Eldar, L. & Harrow, A. W. Local Hamiltonians whose ground states are hard to approximate. ArXiv e-prints (2015). arXiv:1510.02082 [quant-ph].

60. Eisert, J., Cramer, M. & Plenio, M. B. Area laws for the entanglement entropy. *Rev. Mod. Phys.* **82**, 277 (2010).

61. Van den Nest, M., Luttmers, K., Dür, W. & Briegel, H. J. Graph states as ground states of many body spin-1/2 Hamiltonians. *Phys. Rev. A* **77**, 012301 (2008).

62. Renes, J. M., Blume-Kohout, R., Scott, A. J. & Caves, C. M. Symmetric informationally complete quantum measurements. *J. Math. Phys.* **45**, 2171 (2004). quant-ph/0310075.

63. Ahnert, S. E. & Payne, M. C. General implementation of all possible positive-operator-value-. *Phys. Rev. A* **71**, 012330 (2005).

64. Ananth, N. & Senthilvelan, M. Identifying non-k-separability of a class of N-qubit complete graph states using correlation tensors. *Eur. Phys. J. D.* **70**, 149 (2016).

65. Dutta, A., Ryu, J., Laskowski, W. & Źukowski, M. Entanglement criteria for noise resistance of two-qudit states. *Phys. Lett. A* **380**, 2191 (2016).

66. Tóth, G. & Gühne, O. Entanglement detection in the stabilizer formalism. *Phys. Rev. A* **72**, 022340 (2005).



Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this license, visit <http://creativecommons.org/licenses/by/4.0/>.

© The Author(s) 2018