PHYSICAL REVIEW A **92**, 050301(R) (2015)

Quantum entanglement from random measurements

Minh Cong Tran,[1] Borivoje Dakić,[2,3] François Arnault,[4] Wiesław Laskowski,[5] and Tomasz Paterek[1,6,7]
[1]*School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore*
[2]*Faculty of Physics, University of Vienna, Boltzmanngasse 5, A-1090 Vienna, Austria*
[3]*Institute for Quantum Optics and Quantum Information, Austrian Academy of Sciences, Boltzmanngasse 3, A-1090 Vienna, Austria*
[4]*Université de Limoges, 123 avenue A. Thomas, 87060 Limoges CEDEX, France*
[5]*Institute of Theoretical Physics and Astrophysics, University of Gdańsk, PL-80-952 Gdańsk, Poland*
[6]*Centre for Quantum Technologies, National University of Singapore, Singapore*
[7]*MajuLab, CNRS-UNS-NUS-NTU International Joint Research Unit, UMI 3654, Singapore*
(Received 29 December 2014; revised manuscript received 6 October 2015; published 3 November 2015)

We show that the expectation value of squared correlations measured along random local directions is an identifier of quantum entanglement in pure states, which can be directly experimentally assessed if two copies of the state are available. Entanglement can therefore be detected by parties who do not share a common reference frame and whose local reference frames, such as polarizers or Stern-Gerlach magnets, remain unknown. Furthermore, we also show that in every experimental run, access to only one qubit from the macroscopic reference is sufficient to identify entanglement, violate a Bell inequality, and, in fact, observe all phenomena observable with macroscopic references. Finally, we provide a state-independent entanglement witness solely in terms of random correlations and emphasize how data gathered for a single random measurement setting per party reliably detects entanglement. This is only possible due to utilized randomness and should find practical applications in experimental confirmation of multiphoton entanglement or space experiments.

DOI: 10.1103/PhysRevA.92.050301 PACS number(s): 03.67.Mn, 03.65.Ud

I. INTRODUCTION

Quantum mechanics imposes no limits on the spatial separation between entangled particles. This naturally leads one to ask whether observers that have never met and do not share a common reference frame can still detect effects of quantum entanglement. One can further ask if in every experimental run each observer's local reference frame needs to be composed of a huge number of somewhat correlated elementary systems (as is the case for Stern-Gerlach magnets, polarizers, etc.), or if the effects of entanglement can be detected with references composed of only a few systems.

Individually, both of these questions have been addressed before. It is known that entanglement can be detected, cryptography can be realized, and Bell inequalities can be violated without a shared reference frame [1–13], and nonclassical correlations can also be observed with finite-size references which are to some degree correlated [14–16]. Here we simultaneously address both questions and show that observers who have independent reference frames in an unknown state can each use a single spin $\frac{1}{2}$ of the reference per experimental run in order to detect entanglement. If the state of the reference can be controlled, a single spin $\frac{1}{2}$ of it per experimental run will be shown to be sufficient to observe all phenomena that one can observe with macroscopic references in every experimental run.

These findings have both practical and fundamental aspects. On the practical side, they show that entanglement detection is possible with independent reference frames and hence observers can save on communication resources [17–20] or preestablished quantum entanglement [21,22] that would have to be consumed to correlate local reference frames. On the fundamental side, bounded reference frames were discussed in the context of a quantum-to-classical transition [14], where it was noted that the lack of perfect reference frames leads to "intrinsic decoherence" [23–25] that might wash out all quantum features. The present work shows that even a single qubit of a reference frame per experimental run can be used to observe Bell violation and hence reveal quantumness.

II. EXPERIMENTAL SCENARIO

Consider an experiment depicted in Fig. 1. In a single experimental run, the nth party makes use of just two qubits: one from the principal system whose entanglement is going to be estimated, and one reference qubit prepared in an *unknown* pure state with Bloch vector $\vec{u}_n$ (measurement setting). In order to violate a Bell inequality or detect entanglement, certain expectation values have to be estimated which require repeated measurements with the same setting. This can be realized with the help of spontaneous magnetization [26]. Each party prepares a magnetic material that is cooled down below the Curie temperature and becomes ferromagnetic. Spontaneous symmetry breaking causes all of the spins of the material to point in the same randomly oriented direction, allowing observers to use them one by one as reference qubits. The number of spins in a magnet gives the number of experiments, K, with fixed settings $\vec{u}_n$. For the moment, we keep $K \to \infty$, and analyze the effect of finite K at the end of this Rapid Communication.

In each experimental run, every party performs locally a total-spin measurement on the two available qubits. The two possible outcomes correspond to the two qubits in the singlet state, $|\psi^-\rangle\langle\psi^-|$, in which case the observer assigns outcome -3, or to a state in the triplet subspace, $\mathbb{1} - |\psi^-\rangle\langle\psi^-|$, in which case the observer assigns outcome $+1$. Altogether, the quantum-mechanical observable of the nth party is given by

$$(\mathbb{1} - |\psi^-\rangle\langle\psi^-|) - 3|\psi^-\rangle\langle\psi^-| = \sum_{j=x,y,z} \sigma_j \otimes \sigma_j, \quad (1)$$

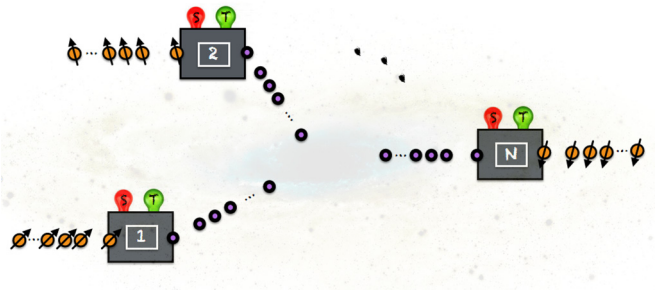

FIG. 1. (Color online) Entanglement detection with minimal independent reference frames. In every experimental run, each observer, enumerated from 1 to N, receives one qubit from a principal system (violet) and takes one qubit from the ensemble of identically aligned reference qubits (orange). The reference qubits are all in the same unknown random state obtained, e.g., by cooling a magnetic material below the Curie temperature. Different observers have independent reference qubits so they can be placed even in far away arms of the galaxy. We show that correlations between results of local total-spin measurements with outcomes denoted by S and T detect quantum entanglement for the principal system in an arbitrary pure state and some mixed ones. In principle, this requires infinitely many experimental runs in order to average over random directions and in order to estimate correlation functions for fixed directions, but we also demonstrate that this technique is useful in the presence of finite resources.

where σ_j is the corresponding Pauli matrix. It is now straightforward to verify that the correlation function between results $+1/-3$ obtained on the principal system in arbitrary state ρ and the reference qubits reads

$$E(\vec{u}_1,\ldots,\vec{u}_N) = \sum_{j_1\ldots j_N=x,y,z} T_{j_1\ldots j_N}(\vec{u}_1)_{j_1}\ldots(\vec{u}_N)_{j_N}, \qquad (2)$$

where $T_{j_1\ldots j_N} = \mathrm{Tr}(\rho\sigma_{j_1}\otimes\cdots\otimes\sigma_{j_N})$ are the correlation tensor elements of the state of the principal system and $(\vec{u}_n)_{j_n}$ is the j_nth component of the Bloch vector $\vec{u}_n$. One recognizes that Eq. (2) is exactly the same as the correlation function between the outcomes of dichotomic ±1 observables in the presence of macroscopic reference frames in every experimental run. Therefore, given the ability to prepare (nonrandom) states $\vec{u}_n$, Eq. (2) shows that *all* quantum phenomena involving dichotomic observables on qubits and macroscopic reference frames in every experimental run can also be observed using a single qubit from a macroscopic reference per experimental run and total-spin local observables. In particular, this allows violation of an arbitrary Bell inequality with the single reference qubit per party per experimental run. For comparison, Costa *et al.* concluded that using spin coherent states as references (of the same size for every party) requires a system of dimension six in every experimental run for the violation of the Clauser-Horne-Shimony-Holt inequality, and of dimension four for the Mermin inequalities, in the limit of $N\to\infty$ [14].

III. RANDOM CORRELATIONS

We proceed to show how correlations measured along M sets of random local directions are related to quantum entanglement. We first assume $M\to\infty$, and analyze the effect of finite M at the end of this Rapid Communication.

Let us represent each setting vector $\vec{u}_n$ in spherical coordinates $\vec{u}_n = (\sin\theta_n\cos\phi_n, \sin\theta_n\sin\phi_n, \cos\theta_n)$. We define *random correlations* as the expectation value of squared correlation functions averaged over uniform choices of settings for each individual observer,

$$\mathcal{R} \equiv \frac{1}{(4\pi)^N}\int d\vec{u}_1\ldots\int d\vec{u}_N\ E^2(\vec{u}_1,\ldots,\vec{u}_N), \qquad (3)$$

where $d\vec{u}_n = \sin\theta_n d\theta_n d\phi_n$ is the usual measure on the unit sphere. Instead of averaging over random $\vec{u}_n$, $\mathcal{R}$ can also be estimated from correlations along orthogonal local directions $\vec{x},\vec{y},\vec{z}$. Let us introduce a quantity which we refer to as the *length of correlations*:

$$\mathcal{C} \equiv \sum_{\vec{u}_1,\ldots,\vec{u}_N=\vec{x},\vec{y},\vec{z}} E^2(\vec{u}_1,\ldots,\vec{u}_N). \qquad (4)$$

Since $\mathcal{C}$ is invariant under local unitary operations (local rotations) [27], and the random correlations are the average of $\mathcal{C}$ over random rotations applied to local bases $\vec{x},\vec{y},\vec{z}$, it is merely a mathematical step to obtain

$$\mathcal{R} = \mathcal{C}/3^N, \qquad (5)$$

where the factor of $1/3$ for every observer takes into account the fact that rotating one axis over a 4π solid angle also makes the other two axes rotate over a 4π solid angle. The following theorem shows a universal lower bound on the random correlations in every pure state $|\psi\rangle$ of N qubits.

Theorem 1. For all pure states of N qubits, $\mathcal{R}\geqslant 1/3^N$.

Proof. We shall prove that $\mathcal{C}\geqslant 1$ for all pure states. We begin by artificially introducing a new set of N qubits prepared in the same N-qubit state $|\psi\rangle$. The quantity $\mathcal{C}$ can now be linearized in the larger Hilbert space composed of initial qubits and the new qubits,

$$\mathcal{C} = \langle\psi|\langle\psi|\mathcal{S}|\psi\rangle|\psi\rangle, \qquad (6)$$

where the first ket in $|\psi\rangle|\psi\rangle$ is the state of the initial qubits $1\ldots N$, and the second ket is the state of artificially introduced qubits $1'\ldots N'$. The operator $\mathcal{S}$ acts on $2N$ qubits and is defined as

$$\mathcal{S} \equiv \sum_{j_1,\ldots,j_N=x,y,z} \sigma_{j_1}^{(1)}\otimes\cdots\otimes\sigma_{j_N}^{(N)}\otimes\sigma_{j_1}^{(1')}\otimes\cdots\otimes\sigma_{j_N}^{(N')}, \qquad (7)$$

where we have explicitly written the qubits on which the Pauli operators act. In order to prove the thesis, we study the eigenproblem of $\mathcal{S}$ and restrict the solutions to the subspace which is symmetric under exchange of the primed and unprimed systems. Let us put $\mathcal{S}$ in the following form:

$$\mathcal{S} = H_{11'}\otimes\cdots\otimes H_{NN'}, \qquad (8)$$

where we introduce the Heisenberg Hamiltonian (in units of coupling strength),

$$H_{nn'} = \sum_{j_n=x,y,z}\sigma_{j_n}^{(n)}\otimes\sigma_{j_n}^{(n')}, \qquad (9)$$

with eigenstates $|00\rangle$, $|11\rangle$, $|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle+|10\rangle)$ (belonging to eigenvalue $+1$), and $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle-|10\rangle)$ (belonging to eigenvalue -3). The eigenvalues of $\mathcal{S}$ are the products

of these eigenvalues. Note, however, that not all such products are allowed if we restrict ourselves to the symmetric subspace. Only the eigenstates with an even number of singlet states $|\psi^-\rangle$ span the symmetric subspace. Therefore, the allowed eigenvalues of $\mathcal{S}$ are given by

$$s_k = (-3)^{2k}, \tag{10}$$

where $2k$ gives the number of singlet pairs. The lowest eigenvalue, $s_0 = 1$, corresponds to no singlets, and we conclude the proof by noting that the expectation value of $\mathcal{S}$ cannot be smaller than the minimal eigenvalue. ■

Our method of proof reveals that random correlations can be directly estimated from a measurement of $\mathcal{S}$ performed on two copies of the quantum state. This is reminiscent of direct entanglement detection schemes using the two copies [28–32] and suggests a deeper link between random correlations and entanglement.

IV. RANDOM CORRELATIONS AND ENTANGLEMENT

The length of correlations $\mathcal{C}$ and similar quantities have appeared in the literature on entanglement detection and quantification before [33–37]. In particular, Hassan and Joag already concluded that $\mathcal{C}$ identifies entanglement in pure states [35]. However, since their derivation relies on an incorrect theorem in Ref. [33], which does not seem to be easily fixable [42], we give an alternative proof utilizing our Theorem 1.

Theorem 2. A pure state is entangled iff $\mathcal{R} > 1/3^N$.

Proof. Clearly, for any product state, we have $\mathcal{R} = 1/3^N$ (and $\mathcal{C} = 1$). For the converse statement, assume that state $|\psi\rangle$ admits $\mathcal{C} = 1$ and decompose it in the standard basis,

$$|\psi\rangle = \sum_{j_1, j_2, \ldots, j_N = 0}^{1} \alpha_{j_1 j_2 \ldots j_N} |j_1\rangle |j_2\rangle \ldots |j_N\rangle. \tag{11}$$

Since $\mathcal{C} = 1$, two copies of $|\psi\rangle$, i.e., $|\psi\rangle \otimes |\psi\rangle$, lie in the subspace spanned by the tensor product of the symmetric states $|00\rangle$, $|11\rangle$, and $|\psi^+\rangle$ only. Therefore, exchanging any qubit i with its hypothetical copy i' will result in the same state. For $i = 1$, this leads to the relation

$$\alpha_{j_1 j_2 .. j_N} \alpha_{j_{1'} j_{2'} .. j_{N'}} = \alpha_{j_{1'} j_2 .. j_N} \alpha_{j_1 j_{2'} .. j_{N'}}, \tag{12}$$

for any $j_2, \ldots, j_N, j_{2'}, \ldots, j_{N'} = 0, 1$. If we choose $j_1 = 0, j_{1'} = 1$ and fix $j_i, j_{i'}$ for all $2 \leqslant i \leqslant N$, this relation takes the form

$$\frac{\alpha_{1|J}}{\alpha_{0|J}} = \frac{\alpha_{1|J'}}{\alpha_{0|J'}}, \tag{13}$$

where $J \equiv j_2 j_3 j_4 \ldots j_N$, for any J, J'. Writing $|\psi\rangle$ in this notation, we have

$$|\psi\rangle = \sum_J \alpha_{0|J} (|0\rangle + k_J |1\rangle) \otimes |J\rangle, \tag{14}$$

where $k_J = \alpha_{1|J}/\alpha_{0|J}$ was introduced in (13) and shown to be independent of J, i.e., $k_J = k$. Therefore, the state of the first qubit is the same for every J and we may rewrite $|\psi\rangle$ in a product form,

$$|\psi\rangle = (|0\rangle + k|1\rangle) \otimes \sum_J \alpha_{0|J} |J\rangle \tag{15}$$

$$= |\Phi_1\rangle \otimes |\Phi_{2\ldots N}\rangle, \tag{16}$$

with $|\Phi_1\rangle$ being a pure state of the first qubit and $|\Phi_{2\ldots N}\rangle$ being a pure state of the last $N - 1$ qubits. Note that by construction,

$$1 = \mathcal{C}_{|\psi\rangle} = \mathcal{C}_{|\Phi_1\rangle} \mathcal{C}_{|\Phi_{2\ldots N}\rangle} = \mathcal{C}_{|\Phi_{2\ldots N}\rangle}, \tag{17}$$

where $\mathcal{C}_{|\phi\rangle}$ is the length of correlations calculated for the state $|\phi\rangle$. Thus we can apply induction and, finally, one can write $|\psi\rangle$ fully as a product state. ■

This theorem provides different perspectives on entanglement in pure states. It is well known that entanglement can be verified by studying the entropy of every one-particle subsystem. As just shown, an alternative complete characterization exists, solely in terms of the correlation functions between *all* N observers (no correlations between smaller number of particles enter this characterization). In this sense, entanglement manifests itself in *full correlations*: entangled states are more correlated in random local measurements than product states.

Another characterization of entanglement is implicit in the proofs above. Only for product states is it possible to swap the same subsystem of the principal system and its copy without changing the whole two-copy state. It is also worth emphasizing that entanglement is detected by a two-step averaging procedure: we need to estimate correlation functions, square them, and then average them over random measurement settings.

V. ENTANGLEMENT WITNESS

In principle, to determine $\mathcal{R}$, an infinite number of measurements has to be performed both in terms of K (the resources needed to estimate correlation functions) and in terms of M (the resources needed for averaging over random settings). Recall that each party repeats M times preparation of K reference qubits. We now introduce and study an entanglement witness [38,39] that takes the finiteness of K and M into account. It can also be used to detect entanglement in some mixed states.

Let us denote by $\mathcal{R}_{M,K}$ the random correlations estimated from correlation functions measured along M sets of random directions, each of which is calculated after K experimental runs. Clearly, if both M and K tend to infinity, then $\mathcal{R}_{M,K} \to \mathcal{R}$. We calculate the standard deviation $\Delta_{M,K}$ of the distribution of $\mathcal{R}_{M,K}$ for product states and propose the following entanglement witness:

$$\mathcal{R}_{M,K} > 1/3^N + 2\Delta_{M,K} \quad \Rightarrow \quad \text{likely } \psi \text{ is ent.} \tag{18}$$

Simply put, if the estimated random correlations are far away from what is expected for a product state, we most likely are dealing with an entangled state. Compared to standard witnesses, ours is for random correlations and can be satisfied by separable states, and yet even a single measurement setting may reveal entanglement with high confidence. We now make this statement precise.

We calculate separately the standard deviation due to finite M, Δ_M, and the standard deviation due to finite K, Δ_K. The final variance is $\Delta^2_{M,K} = \Delta^2_M + \Delta^2_K$. Consider first the case of $K \to \infty$. In Appendix A, we prove that the squared correlation of a pure product state of N qubits measured along a random direction is distributed in $[0,1]$ by the density function

$$\chi_N(E^2) = \frac{1}{2^N\sqrt{E^2}} \frac{(-\ln E^2)^{N-1}}{(N-1)!}. \tag{19}$$

Each time a product state is measured with random settings, the squared correlation is picked from this distribution. After M such trials, by the central limit theorem, the average of squared correlations, $\mathcal{R}_M$, will be normally distributed around the mean $\mathcal{R} = 1/3^N$. The standard deviation of this normal distribution, Δ_M, is closely related to the standard deviation Δ of the distribution (19),

$$\Delta_M = \frac{\Delta}{\sqrt{M}} \quad \text{with} \quad \Delta = \sqrt{\frac{1}{5^N} - \frac{1}{9^N}}. \tag{20}$$

For a normal distribution, there is a 95.4% chance that $\mathcal{R}_M$ lies within $2\Delta_M$ from $\mathcal{R}$. Therefore, if the observed value of $\mathcal{R}_M$ is more than $2\Delta_M$ away from $1/3^N$, we are 95.4% sure that the state is entangled. This reliable state-independent entanglement witness also works for some mixed states, as we show in Appendix B.

To approximate the effects of finite K, let us denote by E_K the value of the correlation function estimated from K experimental runs with the same measurement settings. For $K \to \infty$, the estimated E_K tends to E, the quantum-mechanical prediction for a given setting. By the central limit theorem, the distribution of E_K has standard deviation $\sqrt{(1-E^2)/K}$, where $\sqrt{1-E^2}$ is the standard deviation of the binomial distribution of the product of individual measurement results. This distribution can be used to calculate the variance of E^2_K (see Appendix C for details):

$$\Delta^2_K = \frac{2}{MK^2}\left[1 - \frac{2(1-K)}{3^N} + (1-2K)\left(\frac{1}{9^N} - \Delta^2_M\right)\right], \tag{21}$$

where it is also assumed that M is sufficiently big. In general, in order to reveal entanglement, the number of experimental runs has to scale exponentially with the number of qubits N as random correlations of all states are exponentially small, and their standard deviations have to be exponentially small in order to distinguish them from separable states.

Finally, we emphasize that even a single measurement setting per party suffices to confirm entanglement with a high degree of confidence. The probability that a product state has correlation below $c = 1/3^N + \delta_N$ is given by $\int_0^c \chi_N(E^2)dE^2 = \Gamma[N, -\frac{1}{2}\ln(\delta_N)]/(N-1)!$, with Γ being the incomplete gamma function. If we fix the confidence to 95.4% as for the normal distribution, i.e., choose δ_N correspondingly, then we verify numerically that the probability to observe a Greenberger-Horne-Zeilinger (GHZ) correlation revealing entanglement by a single set of settings with this confidence is 26% for $N = 3$, and already 86% for $N = 10$ qubits. Note that this also holds for GHZ states to which local random rotations have been applied, modeling, e.g., polarization of photons propagating through fibers. Our method also opens the door for entanglement verification in multiphoton experiments (see Appendix B for exemplary detection of noisy GHZ entanglement). For example, in the eight-photon setup of Ref. [40], a coincidence click is observed only every 6–7 minutes. We checked that with a single setting per party and $K = 1000$ coincidences (corresponding to about 4.5 days of running the experiment), our method confirms entanglement with confidence 95.4% (80%) with probability 49% (63%). Since this kind of entanglement detection pushes the number of measurement settings to minimum, this method is perfectly suited for entanglement detection in multipartite systems.

VI. HIGHER DIMENSIONS

Although we have explicitly calculated it for qubits, all of our results apply to d-level systems. One simply replaces in our theorems the Pauli matrices with the generators of SU(d). Since there are $d^2 - 1$ such generators, vectors $\vec{u}_n$ have to be extended to $d^2 - 1$ dimensions as well as the corresponding sums over Pauli matrices. By following the same lines of proofs as for qubits, one finds that for all pure states of N qudits,

$$(d^2-1)^N\mathcal{R} = \mathcal{C} \geqslant \left[\frac{d(d-1)}{2}\right]^N, \tag{22}$$

and again the lower bound is achieved only by product states. It is also straightforward to generalize these proofs to subsystems of arbitrary dimensions $d_1, d_2, \ldots, d_N$.

VII. CONCLUSIONS

We showed that pure state entanglement can be solely characterized by correlations between all involved particles and that it can be detected by measurements along random local directions. Simply put, entangled states are more correlated than product states. No shared reference frame is required for entanglement detection and it can even be revealed using only one qubit per experimental run from a reference in an unknown state. Furthermore, correlations measured along *one* random setting per party are shown to reveal entanglement. This randomness empowered entanglement detection works for pure states as well as some mixed states and can be put to practical use in multiparty experiments as well as setups where frame alignment is difficult, e.g., space experiments with photons. We hope that our different perspective on such a basic aspect of quantum physics as pure state entanglement will find new applications and stimulate new results in all fields that utilize it.

ACKNOWLEDGMENTS

We thank Časlav Brukner for discussions. This work is supported by the National Research Foundation, Ministry of Education of Singapore Grant No. RG98/13, NCN Grant No. 2012/05/E/ST2/02352, European Commission Project RAQUEL, and Austrian Science Fund (FWF) Individual Project No. 2462.

APPENDIX A: DISTRIBUTION OF RANDOM SQUARED CORRELATION OF PRODUCT STATES

Here we show how E^2 of a product state of N qubits is distributed if the measurement direction is chosen uniformly at random. We proceed by induction on the number of qubits. For $N = 1$, without loss of generality we choose the measured state to be $\rho = |0\rangle\langle 0|$. Arbitrary measurement is parameterized by spherical angles (θ,ϕ) and expressed in terms of Pauli matrices as

$$\sigma(\theta,\phi) = \sin\theta\cos\phi\,\sigma_x + \sin\theta\sin\phi\,\sigma_y + \cos\theta\,\sigma_z. \quad \text{(A1)}$$

The squared correlation measured along the direction (θ,ϕ) is therefore

$$E_1^2 = \cos^2\theta, \quad \text{(A2)}$$

where index 1 emphasizes that only one particle is measured. Since the measurement direction is uniformly distributed in a unit spherical shell, $\cos\theta$ is uniformly distributed on $[-1,1]$. From Eq. (A2), the probability density for $E_1^2 \in [0,1]$ is derived to read

$$\chi_1\left(E_1^2\right) = \frac{1}{2\sqrt{E_1^2}}. \quad \text{(A3)}$$

Now we prove that for product states of N qubits squared correlation measured along uniformly random local directions, $E_N^2 \in [0,1]$, is distributed according to probability density

$$\chi_N\left(E_N^2\right) = \frac{1}{2^N\sqrt{E_N^2}}\frac{\left(-\ln E_N^2\right)^{N-1}}{(N-1)!}. \quad \text{(A4)}$$

For $N = 1$, one verifies that (A4) returns (A3). Now assume that (A4) holds for $N = k \geqslant 1$. We shall prove that it holds for $N = k+1$ as well. For a product state of $k+1$ qubits, the correlation factors into the product of correlation for the first k qubits and suitable Bloch component of the state of the last qubit,

$$E_{k+1}^2 = E_k^2\,E_1^2. \quad \text{(A5)}$$

Since now random variable E_{k+1}^2 is a product of two independent random variables E_k^2 and E_1^2, the probability density of E_{k+1}^2 can be calculated as [41]

$$\begin{aligned}\chi_{k+1}\left(E_{k+1}^2\right) &= \int_{E_{k+1}^2}^1 \chi_1(E_1^2)\chi_k\left(\frac{E_{k+1}^2}{E_1^2}\right)\frac{dE_1^2}{E_1^2} \\ &= \frac{1}{2^{k+1}\sqrt{E_{k+1}^2}}\frac{\left(-\ln E_{k+1}^2\right)^k}{k!}, \end{aligned} \quad \text{(A6)}$$

where the lower limit in the integral follows from $E_k^2 = E_{k+1}^2/E_1^2 \leqslant 1$. Thus, (A4) holds for $N = k+1$, and by induction on N, it holds for the product state of any number of qubits. Using this density function, it is straightforward to compute the standard deviation,

$$\Delta = \sqrt{\langle E^4\rangle - \langle E^2\rangle^2} = \sqrt{\frac{1}{5^N} - \frac{1}{9^N}}. \quad \text{(A7)}$$

APPENDIX B: CONVEXITY AND BOUND ON STANDARD DEVIATION OF SEPARABLE STATES

It is difficult to obtain standard deviation similar to (A7) for general separable states. However, we can put an upper bound on it. Let ρ be a separable state

$$\rho = \sum_i p_i\rho_i, \quad \text{(B1)}$$

with pure product states ρ_i of N qubits and probabilities p_i. The correlation of ρ is

$$E(\rho) = \sum_i p_i E(\rho_i). \quad \text{(B2)}$$

Since E^4 is a convex function, $E^4(\rho) \leqslant \sum_i p_i E^4(\rho_i)$, we have

$$\begin{aligned}\Delta_\rho &= \sqrt{\langle E^4\rangle - \langle E^2\rangle^2} \\ &\leqslant \sqrt{\sum_i p_i\langle E^4(\rho_i)\rangle} = \sqrt{\frac{1}{5^N}\sum_i p_i} = \frac{1}{5^{N/2}}. \end{aligned} \quad \text{(B3)}$$

Here, Δ_ρ is the standard deviation of the distribution of squared random correlations of ρ. Since random correlation is a convex function, $\mathcal{R}(\rho) \leqslant \sum_i p_i\mathcal{R}(\rho_i) = 1/3^N$, we are at least 95.4% sure that a mixed states ρ is entangled once its random correlation $\mathcal{R}_\rho$ exceeds the threshold $1/3^N$ by twice the value of $1/5^{N/2}$. To demonstrate this idea, consider an N-qubit mixture of the GHZ state and white noise,

$$\rho = \varepsilon\,\rho_{\mathrm{GHZ}} + (1-\varepsilon)\frac{1}{2^N}\mathbb{I}. \quad \text{(B4)}$$

It is straightforward to verify that the random correlation of such state is given by

$$\mathcal{R}_\rho \simeq \varepsilon^2\frac{2^{N-1}}{3^N}. \quad \text{(B5)}$$

Our witness reveals entanglement in ρ for $\varepsilon \gtrsim \sqrt{\frac{3^N}{2^{N-2}5^{N/2}}}$, i.e., for exponentially small in the number of qubits admixture of the GHZ state.

APPENDIX C: STANDARD DEVIATION OF RANDOM CORRELATION DUE TO FINITE K

Here we derive the standard deviation of random correlation due to a finite number of experimental runs with fixed settings, K, and due to a finite (but large) number of random settings, M. In the main text, we argue that the standard deviation of correlations estimated after K measurement runs for a fixed, say ith, set of settings equals $\sigma_{\varepsilon_i} = \sqrt{(1-\varepsilon_i^2)/K}$, where ε_i denotes the quantum-mechanical correlation function for the ith settings. For finite K, the estimated expectation value (denoted by x) will be normally distributed around ε_i within the range from -1 to $+1$. We assume that ε_i is sufficiently small and/or K is sufficiently large so that the range of the normal distribution is well within $[-1,1]$. Then the probability density of this distribution can be written as

$$f(x) = \frac{1}{\sqrt{2\pi\sigma_{\varepsilon_i}^2}}\exp\left[-\frac{(x-\varepsilon_i)^2}{2\sigma_{\varepsilon_i}^2}\right]. \quad \text{(C1)}$$

The variance of squared correlations follows from the following calculations:

$$\langle x^2\rangle = \int_{-\infty}^{\infty} f(x)x^2dx = \varepsilon_i^2 + \sigma_{\varepsilon_i}^2, \tag{C2}$$

$$\langle x^4\rangle = \int_{-\infty}^{\infty} f(x)x^4dx = \varepsilon_i^4 + 6\varepsilon_i^2\sigma_{\varepsilon_i}^2 + 3\sigma_{\varepsilon_i}^4, \tag{C3}$$

$$\Delta_i^2 \equiv \langle x^4\rangle - \langle x^2\rangle^2 = 2\sigma_{\varepsilon_i}^2\left(\sigma_{\varepsilon_i}^2 + 2\varepsilon_i^2\right) \tag{C4}$$

$$= \frac{2}{K^2}\left(1-\varepsilon_i^2\right)\left(1-\varepsilon_i^2+2K\varepsilon_i^2\right) \tag{C5}$$

$$= \frac{2}{K^2}\left[1-2(1-K)\varepsilon_i^2+(1-2K)\varepsilon_i^4\right]. \tag{C6}$$

Random correlations are additionally averaged over random measurement directions,

$$\mathcal{R}_{M,K} = \frac{1}{M}\left(\varepsilon_1^2+\cdots+\varepsilon_M^2\right). \tag{C7}$$

The variance of random correlation is therefore given by

$$\Delta_K^2 = \frac{1}{M^2}\sum_{i=1}^{M}\Delta_i^2 \tag{C8}$$

$$= \frac{2}{MK^2}\left[1-2(1-K)\sum_i\frac{\varepsilon_i^2}{M}+(1-2K)\sum_i\frac{\varepsilon_i^4}{M}\right] \tag{C9}$$

$$\approx \frac{2}{MK^2}\left[1-\frac{2(1-K)}{3^N}+(1-2K)\left(\frac{1}{9^N}-\Delta_M^2\right)\right], \tag{C10}$$

where in the last line we assume that M is large enough so that for product states $\sum_{i=1}^{M}\frac{\varepsilon_i^2}{M}\to\frac{1}{3^N}$ because it is the expectation value of squared correlations along random directions and $\sum_{i=1}^{M}\frac{\varepsilon_i^4}{M}\to\frac{1}{9^N}+\Delta_M^2$, with Δ_M^2 derived in the main text.

[1] Y.-C. Liang, N. Harrigan, S. D. Bartlett, and T. Rudolph, Phys. Rev. Lett. **104**, 050401 (2010).
[2] J. J. Wallman, Y.-C. Liang, and S. D. Bartlett, Phys. Rev. A **83**, 022110 (2011).
[3] S. D. Bartlett, T. Rudolph, and R. W. Spekkens, Rev. Mod. Phys. **79**, 555 (2007).
[4] J. J. Wallman and S. D. Bartlett, Phys. Rev. A **85**, 024101 (2012).
[5] P. Shadbolt, T. Vertesi, Y.-C. Liang, C. Branciard, N. Brunner, and J. L. O'Brien, Sci. Rep. **2**, 470 (2012).
[6] M. S. Palsson, J. J. Wallman, A. J. Bennet, and G. J. Pryde, Phys. Rev. A **86**, 032322 (2012).
[7] W. Laskowski, D. Richart, C. Schwemmer, T. Paterek, and H. Weinfurter, Phys. Rev. Lett. **108**, 240501 (2012).
[8] W. Laskowski, C. Schwemmer, D. Richart, L. Knips, T. Paterek, and H. Weinfurter, Phys. Rev. A **88**, 022327 (2013).
[9] T. Lawson, A. Pappa, B. Bourdoncle, I. Kerenidis, D. Markham, and E. Diamanti, Phys. Rev. A **90**, 042336 (2014).
[10] C. Furkan Senel, T. Lawson, M. Kaplan, D. Markham, and E. Diamanti, Phys. Rev. A **91**, 052118 (2015).
[11] A. Laing, V. Scarani, J. G. Rarity, and J. L. O'Brien, Phys. Rev. A **82**, 012304 (2010).
[12] J. A. Slater, C. Branciard, N. Brunner, and W. Tittel, New J. Phys. **16**, 043002 (2014).
[13] J. Wabnig, D. Bitauld, H. W. Li, A. Laing, J. L. O'Brien, and A. O. Niskanen, New J. Phys. **15**, 073001 (2013).
[14] F. Costa, N. Harrigan, T. Rudolph, and Č. Brukner, New J. Phys. **11**, 123007 (2009).
[15] G. A. White, J. A. Vaccaro, and H. M. Wiseman, Phys. Rev. A **79**, 032109 (2009).
[16] T. Paterek, P. Kurzyński, D. K. L. Oi, and D. Kaszlikowski, New J. Phys. **13**, 043027 (2011).
[17] A. Peres and P. F. Scudo, Phys. Rev. Lett. **86**, 4160 (2001).
[18] E. Bagan, M. Baig, A. Brey, R. Munoz-Tapia, and R. Tarrach, Phys. Rev. A **63**, 052309 (2001).
[19] A. Peres and P. F. Scudo, Phys. Rev. Lett. **87**, 167901 (2001).
[20] E. Bagan, M. Baig, and R. Munoz-Tapia, Phys. Rev. Lett. **87**, 257903 (2001).
[21] A. Acin, E. Jane, and G. Vidal, Phys. Rev. A **64**, 050302 (2001).
[22] R. Jozsa, D. S. Abrams, J. P. Dowling, and C. P. Williams, Phys. Rev. Lett. **85**, 2010 (2000).
[23] S. D. Bartlett, T. Rudolph, R. W. Spekkens, and P. S. Turner, New J. Phys. **8**, 58 (2006).
[24] D. Poulin, Int. J. Theor. Phys. **45**, 1189 (2006).
[25] R. Gambini, R. A. Porto, and J. Pullin, Phys. Rev. Lett. **93**, 240401 (2004).
[26] N. W. Ashcroft and N. D. Mermin, *Solid State Physics* (Cengage Learning, Boston, 1976).
[27] K. Nagata, W. Laskowski, M. Wieśniak, and M. Żukowski, Phys. Rev. Lett. **93**, 230403 (2004).
[28] F. Mintert and A. Buchleitner, Phys. Rev. Lett. **98**, 140505 (2007).
[29] S. P. Walborn, P. H. Souto Ribeiro, L. Davidovich, F. Mintert, and A. Buchleitner, Phys. Rev. A **75**, 032338 (2007).
[30] L. Aolita, A. Buchleitner, and F. Mintert, Phys. Rev. A **78**, 022308 (2008).
[31] S. P. Walborn, P. H. S. Ribeiro, L. Davidovich, F. Mintert, and A. Buchleitner, Nature (London) **440**, 1022 (2006).
[32] C. Schmid, N. Kiesel, W. Wieczorek, H. Weinfurter, F. Mintert, and A. Buchleitner, Phys. Rev. Lett. **101**, 260505 (2008).
[33] A. S. M. Hassan and P. S. Joag, Quantum Inf. Comput. **8**, 773 (2008).
[34] Ali Saif M. Hassan and P. S. Joag, Phys. Rev. A **77**, 062334 (2008).
[35] Ali Saif M. Hassan and P. S. Joag, Phys. Rev. A **80**, 042302 (2009).
[36] P. Badziąg, Č. Brukner, W. Laskowski, T. Paterek, and M. Żukowski, Phys. Rev. Lett. **100**, 140403 (2008).
[37] W. Laskowski, M. Markiewicz, T. Paterek, and M. Żukowski, Phys. Rev. A **84**, 062305 (2011).
[38] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A **223**, 1 (1996).
[39] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Rev. Mod. Phys. **81**, 865 (2009).
[40] X.-C. Yao, T.-X. Wang, P. Xu, H. Lu, G.-S. Pan, X.-H. Bao, C.-Z. Peng, C.-Y. Lu, Y.-A. Chen, and J.-W. Pan, Nat. Photon. **6**, 225 (2012).

[41] M. D. Springer, *The Algebra of Random Variables* (Wiley, New York, 1979).

[42] In Proposition 1a of Ref. [33], the claim at the end of the proof, i.e., α_k is allowed to be zero, is incorrect because by their assumption only the correlations between *all* of the subsystems can be taken into account, and $\alpha_k = 0$ means that the kth subsystem is not measured.