# Supplemental Material: Collective randomized measurements in quantum information processing

Satoya Imai,[1,2] Géza Tóth,[3,4,5,6,7] and Otfried Gühne[1]

[1] *Naturwissenschaftlich-Technische Fakultät, Universität Siegen, Walter-Flex-Straße 3, 57068 Siegen, Germany*
[2] *QSTAR, INO-CNR, and LENS, Largo Enrico Fermi, 2, 50125 Firenze, Italy*
[3] *Department of Theoretical Physics, University of the Basque Country UPV/EHU, P.O. Box 644, E-48080 Bilbao, Spain*
[4] *EHU Quantum Center, University of the Basque Country UPV/EHU, Barrio Sarriena s/n, ES-48940 Leioa, Biscay, Spain*
[5] *Donostia International Physics Center (DIPC), P.O. Box 1072, E-20080 San Sebastián, Spain*
[6] *IKERBASQUE, Basque Foundation for Science, E-48009 Bilbao, Spain*
[7] *HUN-REN Wigner Research Centre for Physics, P.O. Box 49, H-1525 Budapest, Hungary*

## Appendix A: Proof of Observation 1

**Observation 1.** *For an $N$-qubit permutationally symmetric state $\varrho$, the first, second, and third moments $\mathcal{J}^{(r)}(\varrho)$ for $r = 1, 2, 3$ completely characterize spin-squeezing entanglement. That is, a constructive procedure for achieving the necessary and sufficient condition is obtained by the moments with the parameters $\alpha = 2/N_2$, $\beta = -2(N-2)/(NN_2)$, $\gamma = -1/[2(N-1)]$ and $N_2 = N(N-1)$.*

*Proof.* In the following, we will first describe the logic of how to prove Observation 1 in the main text and later explain each line step-by-step

$$\begin{aligned}
\varrho_{\mathrm{PS}} \in \mathcal{H}_2^{\otimes N} \text{ is spin squeezed} &\iff \varrho_{ab} \in \mathcal{H}_2^{\otimes 2} \text{ is entangled} && \text{(A1a)}\\
&\iff \varrho_{ab} \notin \mathrm{PPT} && \text{(A1b)}\\
&\iff M \not\geq 0 && \text{(A1c)}\\
&\iff C \not\geq 0 && \text{(A1d)}\\
&\iff \text{obtained from } \mathrm{tr}(C^r) \text{ for } r = 1, 2, 3 && \text{(A1e)}\\
&\iff \text{obtained from } \mathcal{C}^{(r)}(\varrho) \text{ for } r = 1, 2, 3 && \text{(A1f)}\\
&\iff \text{obtained from } \mathcal{J}^{(r)}(\varrho) \text{ for } r = 1, 2, 3. && \text{(A1g)}
\end{aligned}$$

In the first line, we denote an $N$-qubit permutationally symmetric state as $\varrho_{\mathrm{PS}}$ and recall again that it possesses bipartite entanglement or often spin squeezing if and only if any two-qubit reduced state $\varrho_{ab} = \mathrm{tr}_{(a,b)^c}(\varrho_{\mathrm{PS}})$ is entangled for $a, b = 1, 2, \ldots, N$, where $X^c$ is the complement of a set $X$. This has been already discussed in Refs. [62–64]. In the second line, we also recall that any two-qubit state is entangled if and only if it has a negative eigenvalue under partial transposition, that is, it violates the so-called PPT criterion [76, 77].

In the third line, we first recall that any two-qubit state $\varrho_{ab}$ can be written as

$$\varrho_{ab} = \frac{1}{4}\sum_{i,j=0}^{3} m_{ij}\sigma_i \otimes \sigma_j. \tag{A2}$$

Here we note that a two-qubit state $\varrho_{ab}$ is permutationally symmetric and separable (that is, PPT) if and only if it holds that $M \geq 0$, where $M = (m_{ij})$ for $i, j = 0, 1, 2, 3$. In the fourth line, this separability condition is equivalent to $C \geq 0$ for a permutationally symmetric $\varrho_{ab}$. Here the $3 \times 3$ matrix $C = (C_{ij})$ is the Schur complement of the $4 \times 4$ matrix $M$, which is given by $C_{ij} = m_{ij} - m_{i0}m_{0j}$ for $i, j = 1, 2, 3$ since $m_{00} = 1$. For details, see Refs. [54, 66, 67].

In the fifth line, we first discuss the explicit form of the covariance matrix $C$

$$C_{ij} = \mathrm{tr}[\varrho_{ab}\sigma_i \otimes \sigma_j] - \mathrm{tr}[\varrho_a\sigma_i]\mathrm{tr}[\varrho_b\sigma_j] = t_{ij} - a_i a_j, \tag{A3}$$

where $m_{ij} = t_{ij} = t_{ji}$ and $m_{i0} = m_{0i} = a_i$ since $\varrho_{ab}$ is permutationally symmetric. Then, the covariance matrix $C = T - \boldsymbol{a}\boldsymbol{a}^\top$ is symmetric $C = C^\top$, where $T = (t_{ij}) = T^\top$ with the constraint $\mathrm{tr}[T] = \sum_i t_{ii} = 1$ and $\boldsymbol{a} = (a_x, a_y, a_z)$. To proceed, let us remark that the matrix $C$ can be diagonalized by a collective local unitary transformation $V \otimes V$, leads to that $OCO^\top = \mathrm{diag}(c_1, c_2, c_3)$ with a rotation matrix $O \in SO(3)$. In fact, the eigenvalues $c_1, c_2, c_3$ can be found by computing the roots of the characteristic polynomial

$$p_C(\lambda) = \lambda^3 - \mathrm{tr}(C)\lambda^2 + \frac{1}{2}\left[\mathrm{tr}(C)^2 - \mathrm{tr}(C^2)\right]\lambda - \det(C), \tag{A4}$$

where $\mathrm{tr}(C^r)=\sum_{i=1,2,3}c_i^r$ and the $\det(C)$ can be written as

$$\det(C)=\frac{1}{6}\left[\mathrm{tr}(C)^3-3\mathrm{tr}(C)\mathrm{tr}(C^2)+2\mathrm{tr}(C^3)\right]. \tag{A5}$$

That is, knowing the $\mathrm{tr}[C^r]$ for $r=1,2,3$ can enable us to access its eigenvalues and therefore decide whether the matrix $C$ is positive or negative.

In the sixth and seventh lines, it is sufficient to show that $\mathrm{tr}[C^r]$ for $r=1,2,3$ can be obtained from the moments $\mathcal{J}^{(r)}(\varrho)$ in the collective randomized measurements. For the choice $\alpha=2/N_2$, $\beta=-2(N-2)/(NN_2)$, $\gamma=-1/[2(N-1)]$, and $N_2=N(N-1)$, we immediately find that the moments $\mathcal{J}^{(r)}(\varrho)$ can be equal to the moments $\mathcal{C}^{(r)}(\varrho_{ab})$ of the random covariance matrix

$$\mathcal{J}^{(r)}(\varrho)=\mathcal{C}^{(r)}(\varrho_{ab})\equiv\int dU\,[\mathrm{Cov}_U]^r, \tag{A6a}$$

$$\mathrm{Cov}_U=\mathrm{tr}[\varrho_{ab}U^{\otimes 2}\sigma_z\otimes\sigma_z(U^\dagger)^{\otimes 2}]-\mathrm{tr}[\varrho_a U\sigma_z U^\dagger]\mathrm{tr}[\varrho_b U\sigma_z U^\dagger]. \tag{A6b}$$

This results from the fact that $\langle J_z\rangle_U=\frac{N}{2}\mathrm{tr}[\varrho_a U\sigma_z U^\dagger]$ and $\langle J_z^2\rangle_U=\frac{N}{4}+\frac{N(N-1)}{2}\mathrm{tr}[\varrho_{ab}U^{\otimes 2}\sigma_z\otimes\sigma_z(U^\dagger)^{\otimes 2}]$. In the following, we will evaluate the moments $\mathcal{C}^{(r)}(\varrho_{ab})$ and show that they are associated with $\mathrm{tr}[C^r]$.

Let us begin by rewriting the moments $\mathcal{C}^{(r)}(\varrho_{ab})$ as

$$\mathcal{C}^{(r)}(\varrho_{ab})=\frac{1}{4^r}\int dU\left[\sum_{i,j=x,y,z}C_{ij}\,\mathcal{O}_U^{(i)}\mathcal{O}_U^{(j)}\right]^r, \tag{A7}$$

where we define that $\mathcal{O}_U^{(i)}=\mathrm{tr}[\sigma_i U\sigma_z U^\dagger]$. For convenience, we denote that

$$\mathcal{I}^{(1)}(i,j)=\int dU\,\mathcal{O}_U^{(i)}\mathcal{O}_U^{(j)}, \tag{A8a}$$

$$\mathcal{I}^{(2)}(i,j,k,l)=\int dU\,\mathcal{O}_U^{(i)}\mathcal{O}_U^{(j)}\mathcal{O}_U^{(k)}\mathcal{O}_U^{(l)}, \tag{A8b}$$

$$\mathcal{I}^{(3)}(i,j,k,l,m,n)=\int dU\,\mathcal{O}_U^{(i)}\mathcal{O}_U^{(j)}\mathcal{O}_U^{(k)}\mathcal{O}_U^{(l)}\mathcal{O}_U^{(m)}\mathcal{O}_U^{(n)}. \tag{A8c}$$

These integrals are known to be simplified as follows

$$\mathcal{I}^{(1)}(i,j)=\frac{4}{3}\delta_{ij}, \tag{A9a}$$

$$\mathcal{I}^{(2)}(i,j,k,l)=\frac{16}{15}\left(\delta_{ij}\delta_{kl}+\delta_{ik}\delta_{jl}+\delta_{il}\delta_{jk}\right), \tag{A9b}$$

$$\begin{aligned}\mathcal{I}^{(3)}(i,j,k,l,m,n)=\frac{64}{105}\Big\{&\delta_{ij}[\delta_{kl}\delta_{mn}+\delta_{km}\delta_{ln}+\delta_{kn}\delta_{lm}]+\delta_{ik}[\delta_{jl}\delta_{mn}+\delta_{jm}\delta_{ln}+\delta_{jn}\delta_{lm}]\\&+\delta_{il}[\delta_{jk}\delta_{mn}+\delta_{jm}\delta_{kn}+\delta_{jn}\delta_{km}]+\delta_{im}[\delta_{jk}\delta_{ln}+\delta_{jl}\delta_{kn}+\delta_{jn}\delta_{kl}]\\&+\delta_{in}[\delta_{jk}\delta_{lm}+\delta_{jl}\delta_{km}+\delta_{jm}\delta_{kl}]\Big\},\end{aligned} \tag{A9c}$$

where we use the formulas in Ref. [10]. Substituting the above results into the moments in Eq. (A7) for different $r=1,2,3$, we can straightforwardly obtain the following expressions

$$\mathcal{C}^{(1)}(\varrho_{ab})=\frac{1}{3}\mathrm{tr}(C), \tag{A10a}$$

$$\mathcal{C}^{(2)}(\varrho_{ab})=\frac{1}{15}\left[\mathrm{tr}(C)^2+\mathrm{tr}(CC^\top)+\mathrm{tr}(C^2)\right], \tag{A10b}$$

$$\mathcal{C}^{(3)}(\varrho_{ab})=\frac{1}{105}\left\{\mathrm{tr}(C)\left[\mathrm{tr}(C)^2+3\mathrm{tr}(C^2)+3\mathrm{tr}(CC^\top)\right]+4\mathrm{tr}(C^2C^\top)+2\mathrm{tr}(CC^\top C^\top)+2\mathrm{tr}(C^3)\right\}. \tag{A10c}$$

Furthermore, using the symmetric condition $C=C^\top$, we can finally arrive at

$$\mathcal{C}^{(1)}(\varrho_{ab})=\frac{1}{3}\mathrm{tr}(C), \tag{A11a}$$

$$\mathcal{C}^{(2)}(\varrho_{ab})=\frac{1}{15}\left[\mathrm{tr}(C)^2+2\mathrm{tr}(C^2)\right], \tag{A11b}$$

$$\mathcal{C}^{(3)}(\varrho_{ab})=\frac{1}{105}\left\{\mathrm{tr}(C)\left[\mathrm{tr}(C)^2+6\mathrm{tr}(C^2)\right]+8\mathrm{tr}(C^3)\right\}. \tag{A11c}$$

The moments $\mathcal{C}^{(r)}(\varrho_{ab})$, equivalently $\mathcal{J}^{(r)}(\varrho)$, are directly connected to $\mathrm{tr}[C^r]$. Hence we complete the proof. □

## Appendix B: Derivation of the result in Observation 2

**Observation 2.** *For an $N$-qubit state $\varrho$, the first moment $\mathcal{J}^{(1)}$ with $(\alpha,\beta,\gamma)=(3,0,0)$ is given by*

$$\mathcal{J}^{(1)}(\varrho)=\sum_{l=x,y,z}(\Delta J_l)^2. \tag{B1}$$

*Any $N$-qubit fully separable state obeys*

$$\mathcal{J}^{(1)}(\varrho)\geq\frac{N}{2}. \tag{B2}$$

*Then violation implies the presence of multipartite entanglement.*

*Proof.* Here we give the derivation of Eq. (B1). Let us begin by writing that $\mathcal{J}^{(1)}(\varrho)=3\int dU\,(\Delta J_z)^2_U$ and

$$\begin{aligned}(\Delta J_z)^2_U&=\langle U^{\otimes N}J_z^2(U^\dagger)^{\otimes N}\rangle_\varrho-\langle U^{\otimes N}J_z(U^\dagger)^{\otimes N}\rangle_\varrho^2\\&=\frac{1}{4}\sum_{i,j=1}^N\langle U^{\otimes N}\sigma_z^{(i)}\otimes\sigma_z^{(j)}(U^\dagger)^{\otimes N}\rangle_\varrho-\frac{1}{4}\sum_{i,j=1}^N\langle U^{\otimes N}\sigma_z^{(i)}(U^\dagger)^{\otimes N}\rangle_\varrho\langle U^{\otimes N}\sigma_z^{(j)}(U^\dagger)^{\otimes N}\rangle_\varrho\\&=\frac{1}{4}\left\{N+\sum_{i\neq j}^N\mathrm{tr}\left[U^{\otimes 2}\sigma_z^{(i)}\otimes\sigma_z^{(j)}(U^\dagger)^{\otimes 2}\varrho_{ij}\right]-\sum_{i,j=1}^N\mathrm{tr}\left[U\sigma_z^{(i)}U^\dagger\varrho_i\right]\mathrm{tr}\left[U\sigma_z^{(j)}U^\dagger\varrho_j\right]\right\},\end{aligned} \tag{B3}$$

where $\varrho_{ij}$ and $\varrho_i$ are the two-qubit and single-qubit reduced states of $\varrho$. Let us focus on the second term in Eq. (B3) and take the Haar unitary average

$$\begin{aligned}\sum_{i\neq j}^N\int dU\,\mathrm{tr}\left[U^{\otimes 2}\sigma_z^{(i)}\otimes\sigma_z^{(j)}(U^\dagger)^{\otimes 2}\varrho_{ij}\right]&=\frac{1}{4}\sum_{i\neq j}^N\int dU\,\mathrm{tr}\left[U^{\otimes 2}\sigma_z^{(i)}\otimes\sigma_z^{(j)}(U^\dagger)^{\otimes 2}\sum_{k,l=x,y,z}t_{kl}^{(i,j)}\sigma_k^{(i)}\otimes\sigma_l^{(j)}\right]\\&=\frac{1}{4}\sum_{i\neq j}^N\sum_{k,l=x,y,z}t_{kl}^{(i,j)}\int dU\,\mathrm{tr}\left[U\sigma_z^{(i)}U^\dagger\sigma_k^{(i)}\right]\mathrm{tr}\left[U\sigma_z^{(j)}U^\dagger\sigma_l^{(j)}\right]\\&=\frac{1}{3}\sum_{i\neq j}^N\sum_{l=x,y,z}t_{ll}^{(i,j)}=\frac{4}{3}\sum_{l=x,y,z}\langle J_l^2\rangle-N,\end{aligned} \tag{B4}$$

where $t_{kl}^{(i,j)}=\langle\sigma_k^{(i)}\otimes\sigma_l^{(j)}\rangle_{\varrho_{ij}}$. Similarly, the third term in Eq. (B3) can be given by

$$\sum_{i,j=1}^N\int dU\,\mathrm{tr}\left[U\sigma_z^{(i)}U^\dagger\varrho_i\right]\mathrm{tr}\left[U\sigma_z^{(j)}U^\dagger\varrho_j\right]=\frac{4}{3}\sum_{l=x,y,z}\langle J_l\rangle^2. \tag{B5}$$

Summarizing these results, we can thus arrive at

$$\mathcal{J}^{(1)}(\varrho)=\frac{3}{4}\left\{N+\frac{4}{3}\sum_{l=x,y,z}\langle J_l^2\rangle-N+\frac{4}{3}\sum_{l=x,y,z}\langle J_l\rangle^2\right\}=\sum_{l=x,y,z}(\Delta J_l)^2. \tag{B6}$$

□

**Remark B1.** Here we consider the generalization of Observation 2 in the main text to high-dimensional spin systems. For that, let us denote the $N$-qudit collective operators $\Lambda_l=\frac{1}{d}\sum_{i=1}^N\lambda_l^{(i)}$, with the so-called Gell-Mann matrices $\lambda_l^{(i)}$ for $l=1,2,\ldots,d^2-1$ acting on $i$-th system. The Gell-Mann matrices are $d$-dimensional extensions of Pauli matrices satisfying the properties: $\lambda_l^\dagger=\lambda_l,\mathrm{tr}(\lambda_l)=0,\mathrm{tr}(\lambda_k\lambda_l)=d\delta_{kl}$. For details, see [107–110]. Let us define the random expectation and its variance

$$\langle\Lambda_l\rangle_U=\mathrm{tr}[\varrho U^{\otimes N}\Lambda_l(U^\dagger)^{\otimes N}],\qquad(\Delta\Lambda_l)^2_U=\langle\Lambda_l^2\rangle_U-\langle\Lambda_l\rangle_U^2, \tag{B7}$$

which depends on the choice of collective unitaries $U^{\otimes N}$ with $U \in \mathcal{U}(d)$. Now we introduce the average of $(\Delta\Lambda_l)^2_U$ for any $l$ over Haar random unitaries

$$\mathcal{D}(\varrho) = (d^2-1)\int dU\,(\Delta\Lambda_l)^2_U. \tag{B8}$$

Now we can make the following:

**Remark B2.** *For an $N$-qudit state $\varrho$, the average can be given by*

$$\mathcal{D}(\varrho) = \sum_{l=1}^{d^2-1}(\Delta\Lambda_l)^2. \tag{B9}$$

*Any $N$-qudit fully separable state obeys*

$$\sum_{l=1}^{d^2-1}(\Delta\Lambda_l)^2 \geq \frac{N(d-1)}{d}. \tag{B10}$$

*This violation implies the presence of multipartite entanglement.*

This is the generalization of Observation 2. The fully separable bound was already discussed in Refs. [111, 112]. In the following, we give the derivation of Eq.(B9).

*Proof.* Similarly to Eq. (B3), the random variance $(\Delta\Lambda_l)^2_U$ can be written as

$$(\Delta\Lambda_l)^2_U = \frac{1}{d^2}\left\{\sum_{i=1}^{N}\mathrm{tr}[U(\lambda_l^{(i)})^2U^\dagger\varrho_i] + \sum_{i\neq j}^{N}\mathrm{tr}\left[U^{\otimes 2}\lambda_l^{(i)}\otimes\lambda_l^{(j)}(U^\dagger)^{\otimes 2}\varrho_{ij}\right] - \sum_{i,j=1}^{N}\mathrm{tr}\left[U\lambda_l^{(i)}U^\dagger\varrho_i\right]\mathrm{tr}\left[U\lambda_l^{(j)}U^\dagger\varrho_j\right]\right\}, \tag{B11}$$

where $\varrho_{ij}$ and $\varrho_i$ are the two-qudit and single-qudit reduced states of $\varrho$. To evaluate the Haar unitary integral, let us use the known formulas [2, 50, 113–117]

$$\int dU\,UXU^\dagger = \frac{\mathrm{tr}[X]}{d}\mathbb{1}_d, \quad \int dU\,U^{\otimes 2}X(U^\dagger)^{\otimes 2} = \frac{1}{d^2-1}\left\{\left[\mathrm{tr}(X) - \frac{\mathrm{tr}(\mathbb{S}X)}{d}\right]\mathbb{1}_d^{\otimes 2} + \left[\mathrm{tr}(\mathbb{S}X) - \frac{\mathrm{tr}(X)}{d}\right]\mathbb{S}\right\}, \tag{B12}$$

for an operator $X$. Here $\mathbb{S}$ is the SWAP (flip) operator acting on $d\times d$-dimensional systems, defined as $\mathbb{S}\,|a\rangle\,|b\rangle = |b\rangle\,|a\rangle$. Thus we first obtain

$$\sum_{i=1}^{N}\int dU\,\mathrm{tr}[U(\lambda_l^{(i)})^2U^\dagger\varrho_i] = \sum_{i=1}^{N}\frac{\mathrm{tr}[(\lambda_l^{(i)})^2]}{d}\mathrm{tr}[\varrho_i] = N. \tag{B13}$$

Next, we have

$$\begin{aligned}
\sum_{i\neq j}^{N}\int dU\,\mathrm{tr}\left[U^{\otimes 2}\lambda_l^{(i)}\otimes\lambda_l^{(j)}(U^\dagger)^{\otimes 2}\varrho_{ij}\right] &= \frac{1}{d^2}\sum_{i\neq j}^{N}\int dU\,\mathrm{tr}\left[U^{\otimes 2}\lambda_l^{(i)}\otimes\lambda_l^{(j)}(U^\dagger)^{\otimes 2}\sum_{m,n=1}^{d^2-1}t_{mn}^{(i,j)}\lambda_m^{(i)}\otimes\lambda_n^{(j)}\right] \\
&= \frac{1}{d^2}\frac{1}{d^2-1}\sum_{i\neq j}^{N}\sum_{m,n=1}^{d^2-1}t_{mn}^{(i,j)}\mathrm{tr}\left[(d\mathbb{S}-\mathbb{1}_d^{\otimes 2})\lambda_m^{(i)}\otimes\lambda_n^{(j)}\right] \\
&= \frac{1}{d^2-1}\sum_{i\neq j}^{N}\sum_{l=1}^{d^2-1}t_{ll}^{(i,j)} \\
&= \frac{d^2}{d^2-1}\sum_{l=1}^{d^2-1}\langle\Lambda_l^2\rangle - N.
\end{aligned} \tag{B14}$$

In the first line, we denote that $t_{mn}^{(i,j)} = \langle\lambda_m^{(i)}\otimes\lambda_n^{(j)}\rangle_{\varrho_{ij}}$. In the second line, we used the formula in Eq. (B12) and the so-called SWAP trick: $\mathrm{tr}[\mathbb{S}X] = \mathrm{tr}[\mathbb{S}(X_A\otimes X_B)] = \mathrm{tr}[X_AX_B]$ for an operator $X = X_A\otimes X_B$. In the final line, we used

that $\sum_{l=1}^{d^2-1}\lambda_l^2=(d^2-1)\mathbb{1}_d$, which can be derived from the facts that $\mathbb{S}=\frac{1}{d}\sum_{l=0}^{d^2-1}\lambda_l\otimes\lambda_l$ and $\mathbb{S}^2=\mathbb{1}_d^{\otimes 2}$. Similarly, we obtain

$$\sum_{i,j=1}^{N}\int dU\,\mathrm{tr}\left[U\lambda_l^{(i)}U^\dagger\varrho_i\right]\mathrm{tr}\left[U\lambda_l^{(j)}U^\dagger\varrho_j\right]=\frac{1}{d^2-1}\sum_{i,j=1}^{N}[d\mathrm{tr}(\varrho_i\varrho_j)-1]=\frac{d^2}{d^2-1}\sum_{l=1}^{d^2-1}\langle\Lambda_l\rangle^2. \tag{B15}$$

Summarizing these results, we can complete the proof. □

## Appendix C: Detailed discussion of Observation 3

**Observation 3.** *The average $\mathcal{T}(\varrho)$ is given by*

$$\mathcal{T}(\varrho)=\mathrm{tr}[\varrho\mathcal{O}_{\mathcal{A}}]=\sum_{i<j<k}\sum_{a,b,c}\varepsilon_{abc}\langle\sigma_a^{(i)}\otimes\sigma_b^{(j)}\otimes\sigma_c^{(k)}\rangle_\varrho, \tag{C1}$$

*where $\varepsilon_{abc}$ denotes the Levi-Civita symbol for $a,b,c=x,y,z$. Any $N$-qubit fully separable state can obey a certain tight bound*

$$|\mathcal{T}(\varrho)|\leq p_{fs}^{(N)}, \tag{C2}$$

*where $p_{fs}^{(N)}$ can be computed analytically for $N=3$ and numerically for up to $N\leq 7$ and is, up to numerical precision, given by $p_{fs}^{(N)}=N^2\cot(\pi/N)/3\sqrt{3}$. Then violation implies the presence of multipartite entanglement.*

*Proof.* Here we give the derivation of Eq. (C1). Let us begin by recalling

$$\mathcal{T}(\varrho)=\int dU\,\mathrm{tr}\left[\varrho U^{\otimes N}\mathcal{O}_{\mathcal{A}}(U^\dagger)^{\otimes N}\right],\qquad \mathcal{O}_{\mathcal{A}}=\sum_{i<j<k}\mathcal{A}\left(\sigma_x^{(i)}\otimes\sigma_y^{(j)}\otimes\sigma_z^{(k)}\right), \tag{C3}$$

where $\mathcal{A}$ represents a linear mapping that can make the antisymmetrization (or alternatization) by summing over even permutations and subtracting the sum over odd permutations. More precisely, the observable can be rewritten as

$$\mathcal{O}_{\mathcal{A}}=\sum_{i<j<k}\sum_{l,m,n=x,y,z}\varepsilon_{lmn}\sigma_l^{(i)}\otimes\sigma_m^{(j)}\otimes\sigma_n^{(k)}. \tag{C4}$$

For instance, in the three-qubit system $ABC$, it is given by

$$\begin{aligned}\mathcal{O}_{\mathcal{A}}=&\sigma_x^{(A)}\otimes\sigma_y^{(B)}\otimes\sigma_z^{(C)}+\sigma_y^{(A)}\otimes\sigma_z^{(B)}\otimes\sigma_x^{(C)}+\sigma_z^{(A)}\otimes\sigma_x^{(B)}\otimes\sigma_y^{(C)}\\&-\sigma_x^{(A)}\otimes\sigma_z^{(B)}\otimes\sigma_y^{(C)}-\sigma_y^{(A)}\otimes\sigma_x^{(B)}\otimes\sigma_z^{(C)}-\sigma_z^{(A)}\otimes\sigma_y^{(B)}\otimes\sigma_x^{(C)}.\end{aligned} \tag{C5}$$

Then we have

$$\begin{aligned}\mathcal{T}(\varrho)&=\sum_{i<j<k}\sum_{l,m,n=x,y,z}\varepsilon_{lmn}\left\{\int dU\,\mathrm{tr}\left[\varrho_{ijk}U^{\otimes 3}\sigma_l^{(i)}\otimes\sigma_m^{(j)}\otimes\sigma_n^{(k)}(U^\dagger)^{\otimes 3}\right]\right\}\\&=\frac{1}{2^3}\sum_{i<j<k}\sum_{l,m,n=x,y,z}\sum_{a,b,c=x,y,z}\varepsilon_{lmn}\xi_{abc}^{(i,j,k)}\int dU\,\mathrm{tr}[\sigma_a^{(i)}U\sigma_l^{(i)}U^\dagger]\mathrm{tr}[\sigma_b^{(j)}U\sigma_m^{(j)}U^\dagger]\mathrm{tr}[\sigma_c^{(k)}U\sigma_n^{(k)}U^\dagger],\end{aligned} \tag{C6}$$

where $\varrho_{ijk}$ is the three-qubit reduced state of $\varrho$ for $i,j,k=1,2,\ldots,N$ with the three-body correlation $\xi_{abc}^{(i,j,k)}=\mathrm{tr}[\varrho_{ijk}\sigma_a^{(i)}\sigma_b^{(j)}\sigma_c^{(k)}]$ for $a,b,c=x,y,z$.

To evaluate the Haar unitary integral, we use the formula

$$\int dU\,\mathrm{tr}[\sigma_aU\sigma_xU^\dagger]\mathrm{tr}[\sigma_bU\sigma_yU^\dagger]\mathrm{tr}[\sigma_cU\sigma_zU^\dagger]=\frac{4}{3}\varepsilon_{abc}, \tag{C7}$$

which has been derived in Ref. [10]. Using this formula leads to

$$\mathcal{T}(\varrho)=\frac{1}{2^3}\frac{4}{3}\sum_{i<j<k}\sum_{l,m,n=x,y,z}\sum_{a,b,c=x,y,z}\varepsilon_{lmn}\xi_{abc}^{(i,j,k)}\varepsilon_{abc}=\sum_{i<j<k}\sum_{a,b,c=x,y,z}\xi_{abc}^{(i,j,k)}\varepsilon_{abc}. \tag{C8}$$

Hence we can complete the proof. □

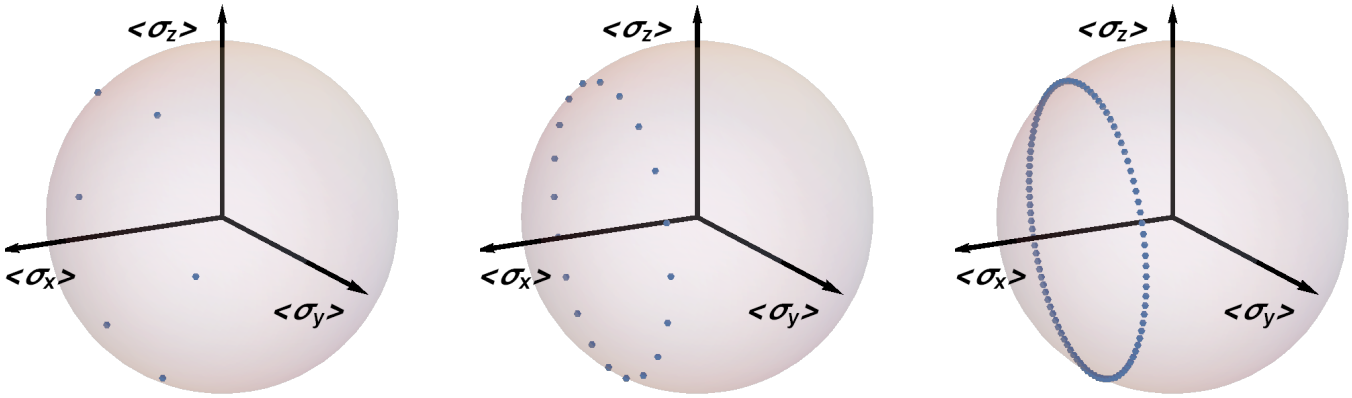


Figure 3. Geometry of $N$ single-qubit states $|\chi_i\rangle$ represented as (Blue) points on the surface in the single-qubit Bloch sphere, for $i = 1, 2, \ldots N$ and $N = 6, 20, 100$.

**Remark C1.** Here we explain how to derive the bound $p_{\rm fs}^{(N)}$. First, we note that the average $|\mathcal{T}(\varrho)|$ is a convex function of a quantum state. Then it is enough to maximize the average for all $N$-qubit pure fully separable states: $|\Phi_{\rm fs}\rangle = \bigotimes_{i=1}^{N} |\chi_i\rangle$. Each of single-qubit states $|\chi_i\rangle$ can be mapped into points on the surface in the single-qubit Bloch sphere, which can be parameterized as $\langle\sigma_x\rangle_{\chi_i} = \cos(\theta_i)$, $\langle\sigma_y\rangle_{\chi_i} = \sin(\theta_i)\cos(\phi_i)$, and $\langle\sigma_z\rangle_{\chi_i} = \sin(\theta_i)\sin(\phi_i)$ for $\chi_i = |\chi_i\rangle\langle\chi_i|$. Substituting these expressions into $|\mathcal{T}(\varrho)|$ and performing its maximization over the parameters, we can find the bound $p_{\rm fs}^{(N)}$. From numerical research up to $N \leq 7$, we collect evidence that there may exist the *tight* bound

$$p_{\rm fs}^{(N)} = \frac{N^2 \cot\left(\frac{\pi}{N}\right)}{3\sqrt{3}}, \tag{C9}$$

which may be obtained by $\theta_i = 2\tan^{-1}(\sqrt{2-\sqrt{3}})$ and $\phi_i = 2\pi i/N$ for $i = 1, 2, \ldots, N$. In Fig. 3, we illustrate the geometrical expressions of the points $|\chi_i\rangle$ on the surface in the single-qubit Bloch sphere for $N = 6, 20, 100$. Note that we will give the analytical proof of the case with $N = 3$ at **Corollary** in the end of Appendix C.

**Remark C2.** In Fig. 4, we illustrate the criterion of Observation 3 for the state $\varrho_{x,y}$ in Eq. (14) in the main text for $N = 4, 5, 6$ on the $x - y$ plane.

**Remark C3.** Let us generalize Observation 3 in the main text by focusing only on three-particle systems. We begin by denoting three-particle $d$-dimensional (three-qudit) operator as

$$W_S = \sum_{i,j,k} w_{ijk} s_i \otimes s_j \otimes s_k, \tag{C10}$$

for some given three-fold tensor $w_{ijk}$ and matrices $s_i \in \mathcal{H}_d$ with $s_i \neq \mathbb{1}_d$. If $d = 2$, $w_{ijk} = \varepsilon_{ijk}$, and $s_i = \sigma_i$, then it holds that $|\langle W_S\rangle| = |\mathcal{T}|$. To proceed, we recall that a three-particle state is called biseparable if

$$\varrho_{\rm bs} = \sum_k p_k^A \varrho_k^A \otimes \varrho_k^{BC} + \sum_k p_k^B \varrho_k^B \otimes \varrho_k^{CA} + \sum_k p_k^C \varrho_k^C \otimes \varrho_k^{AB}, \tag{C11}$$

where and $p_k^X$ for $X = A, B, C$ are probability distributions. The state is called genuinely multiparticle entangled if it cannot be written in the form of $\varrho_{\rm bs}$. Now we will make the following:

**Lemma.** *For a three-qudit state $\varrho_{ABC}$, we denote the vector $\boldsymbol{s}_X = (s_i^X)$ and the matrix $S_{XY} = (s_{ij}^{XY})$ with $s_i^X = \mathrm{tr}[\varrho^X s_i]$ and $s_{ij}^{XY} = \mathrm{tr}[\varrho^{XY} s_i \otimes s_j]$, where $\varrho_X, \varrho_{XY}$ are marginal reduced states of $\varrho_{ABC}$ for $X, Y, Z = A, B, C$. Any three-qudit fully separable state obeys*

$$|\langle W_S\rangle| \leq \max_{X,Y,Z=A,B,C} \|\boldsymbol{s}_X\| \, \|\boldsymbol{v}_{YZ}\|, \tag{C12}$$

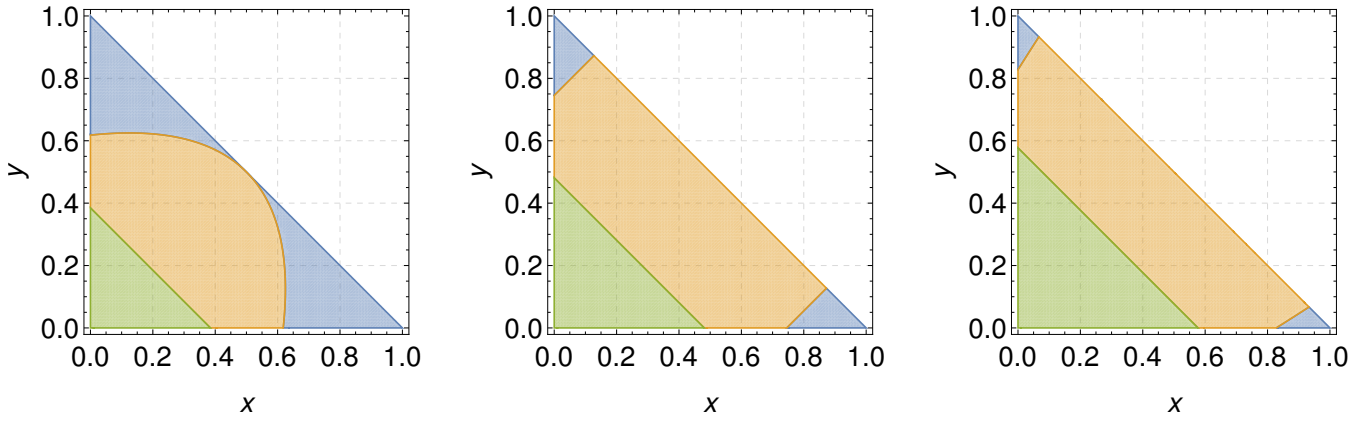


Figure 4. Entanglement criteria for the mixed state in Eq. (14) in the main text for $N = 4, 5, 6$ in the $x - y$ plane. The fully separable states are contained in Green area, which obeys all the optimal spin-squeezing inequalities (OSSIs) previously known with optimal measurement directions [44, 45] and also our criterion in Obs. 3 in the main text. Blue area corresponds to the spin-squeezed entangled states that can be detected by all OSSIs and Obs. 3. Yellow area corresponds to the entangled states that cannot be detected by all OSSIs but can be detected by Obs. 3, thus marking the improvement of this paper compared with previous results.

*where* $\|\boldsymbol{v}\|^2 = \sum_i v_i^2$ *is the Euclidean vector norm of a vector* $\boldsymbol{v}$ *with elements* $v_i$ *and the vector* $\boldsymbol{v}_{YZ} = (v_i^{YZ})$ *with* $v_i^{YZ} = \sum_{j,k} s_j^Y s_k^Z w_{ijk}$. *Also, any three-qudit biseparable state obeys*

$$|\langle W_S\rangle| \leq \max_{X,Y,Z=A,B,C} \sum_i \sigma_i(S_{XY})\sigma_i(Z^*), \tag{C13}$$

*where* $\sigma_i(O)$ *are singular values of a matrix* $O$ *in decreasing order and the matrix* $Z^* = (z_{ij}^*)$ *with* $z_{ij}^* = \sum_k s_k^Z w_{ijk}$.

*Proof.* Since $|\langle W_S\rangle|$ is a convex function for a state, it is sufficient to prove the cases of pure states. First, let us consider a pure fully separable state $\varrho^A \otimes \varrho^B \otimes \varrho^C$. Then we have

$$\langle W_S\rangle = \sum_{i,j,k} w_{ijk}\mathrm{tr}[\varrho^A \otimes \varrho^B \otimes \varrho^C s_i \otimes s_j \otimes s_k] = \sum_i s_i^A \sum_{j,k} s_j^B s_k^C w_{ijk} = \sum_i s_i^A v_i^{BC} \leq \|\boldsymbol{s}_A\| \, \|\boldsymbol{v}_{BC}\|\,, \tag{C14}$$

where we used the Cauchy–Schwarz inequality to derive the inequality. Similarly, we can have cases that correspond to $\boldsymbol{s}_B$ and $\boldsymbol{s}_C$.

Second, let us consider a pure biseparable state for a fixed bipartition $XY|Z$. For a case $AB|C$, we have

$$\langle W_S\rangle = \sum_{i,j} s_{ij}^{AB} \sum_k s_k^C w_{ijk} = \sum_{i,j} s_{ij}^{AB} c_{ij}^* = \mathrm{tr}[S_{AB}(C^*)^\top] \leq \sum_i \sigma_i(S_{AB})\sigma_i(C^*), \tag{C15}$$

where we used von Neumann's trace inequality [118]. Similarly, we can obtain the bounds for the other bipartitions $B|CA$ and $C|AB$. Hence we can complete the proof. □

**Corollary.** *Consider the case where* $d = 2$, $w_{ijk} = \varepsilon_{ijk}$, *and* $s_i = \sigma_i$. *Any three-qubit fully separable state obeys* $|\langle W_S\rangle| \leq 1$. *Also, any three-qubit biseparable state obeys* $|\langle W_S\rangle| \leq 2$.

*Proof.* To show these, without loss of generality, we can take $\varrho^C = |0\rangle\langle 0|$. This can lead to that $\boldsymbol{v}_{BC} = (s_2^B, -s_1^B, 0)$. For single-qubit pure states, we have that $\|\boldsymbol{s}_A\| = 1$ and $\|\boldsymbol{v}_{BC}\| \leq 1$. Thus we can show the the fully separable bound. For the biseparable bound, since $\sigma_1(C^*) = \sigma_2(C^*) = 1$ and $\sigma_3(C^*) = 0$, we can immediately find that $\sigma_1(S_{AB}) + \sigma_2(S_{AB}) \leq 2$ for all pure $\varrho^{AB}$. □

## Appendix D: Detailed discussion of Observation 4

**Observation 4.** *For a $2N$-qubit state $\varrho_{AB}$ with the permutationally symmetric reduced states, any separable $\varrho_{AB}$ obeys*

$$\mathcal{G}_{AB}^{(2)} + \mathcal{J}_A^{(1)} + \mathcal{J}_B^{(1)} - \mathcal{J}_A^{(1)}\mathcal{J}_B^{(1)} \leq 1, \tag{D1}$$

*where $g = (3/N^2)^2$ and $(\alpha, \beta, \gamma) = (0, 12/N^2, 0)$.*

*Proof.* We begin by writing

$$\mathcal{G}_{AB}^{(r)} = g \int dU_A \int dU_B \, [\eta_{U_{AB}}]^r, \qquad \eta_{U_{AB}} = (\Delta J_z^+)_{U_{AB}}^2 - (\Delta J_z^-)_{U_{AB}}^2, \tag{D2a}$$

$$\mathcal{J}_X^{(r)}(\varrho_X) = \int dU_X \, [f_U(\varrho_X)]^r, \qquad f_U(\varrho_X) = \alpha(\Delta J_{z,X})_{U_X}^2 + \beta\langle J_{z,X}\rangle_{U_X}^2 + \gamma, \tag{D2b}$$

where

$$\langle J_z^\pm\rangle_{U_{AB}} = \mathrm{tr}\left[\varrho_{AB} U_{AB}^{\otimes N} J_z^\pm (U_{AB}^\dagger)^{\otimes N}\right], \qquad (\Delta J_z^\pm)_{U_{AB}}^2 = \langle (J_z^\pm)^2\rangle_{U_{AB}} - \langle J_z^\pm\rangle_{U_{AB}}^2, \tag{D3a}$$

$$J_z^\pm = J_{z,A} \pm J_{z,B}, \qquad J_{z,X} = \frac{1}{2}\sum_{i=1}^N \sigma_z^{(X_i)}, \qquad U_{AB} = U_A \otimes U_B. \tag{D3b}$$

Then we can have

$$\langle J_z^\pm\rangle_{U_{AB}}^2 = \langle J_{z,A}\rangle_{U_A}^2 + \langle J_{z,B}\rangle_{U_B}^2 \pm 2\langle J_{z,A}\rangle_{U_A}\langle J_{z,B}\rangle_{U_B}, \tag{D4a}$$

$$(\Delta J_z^\pm)_{U_{AB}}^2 = (\Delta J_{z,A})_{U_A}^2 + (\Delta J_{z,B})_{U_B}^2 \pm 2\left[\langle J_{z,A}\otimes J_{z,B}\rangle_{U_{AB}} - \langle J_{z,A}\rangle_{U_A}\langle J_{z,B}\rangle_{U_B}\right], \tag{D4b}$$

$$\eta_{U_{AB}} = 4\left[\langle J_{z,A}\otimes J_{z,B}\rangle_{U_{AB}} - \langle J_{z,A}\rangle_{U_A}\langle J_{z,B}\rangle_{U_B}\right]. \tag{D4c}$$

Let us evaluate the form of $\mathcal{G}_{AB}^{(2)}(\varrho_{AB})$. Applying the assumption that $\varrho_A$ and $\varrho_B$ are permutationally symmetric, we can further simplify the form of $\eta_{U_{AB}}$

$$\begin{aligned}\eta_{U_{AB}} &= 4\frac{1}{2}\frac{1}{2}\left\{\sum_{i,j=1}^N \mathrm{tr}[\varrho_{A_iB_j} U_A \sigma_z^{(A_i)} U_A^\dagger \otimes U_B \sigma_z^{(B_j)} U_B^\dagger] - \sum_{i,j=1}^N \mathrm{tr}[\varrho_{A_i} U_A \sigma_z^{(A_i)} U_A^\dagger]\mathrm{tr}[\varrho_{B_i} U_B \sigma_z^{(B_i)} U_B^\dagger]\right\} \\ &= \frac{N^2}{4}\sum_{p,q=x,y,z} C_{pq}\mathcal{O}_{U_A}^{(p)}\mathcal{O}_{U_B}^{(q)},\end{aligned} \tag{D5}$$

where the covariance matrix $C = (C_{pq})$ is given by

$$C_{pq} = \mathrm{tr}[\varrho_{A_iB_j}\sigma_p^{(A_i)}\otimes\sigma_q^{(B_j)}] - \mathrm{tr}[\varrho_{A_i}\sigma_p^{(A_i)}]\mathrm{tr}[\varrho_{B_j}\sigma_q^{(B_j)}] = t_{pq} - a_p b_q, \tag{D6}$$

for the two-qubit reduced state $\varrho_{A_iB_j} = \mathrm{tr}_{\overline{ij}}(\varrho_{AB})$ such that both particles are still spatially separated, defined in $\mathcal{H}_{A_i}\otimes\mathcal{H}_{B_j}$. Here we denote that

$$\mathcal{O}_{U_X}^{(p)} = \mathrm{tr}\left[\sigma_p^{(X_i)} U_X \sigma_z^{(X_i)} U_X^\dagger\right], \tag{D7}$$

for $X_i = A_i, B_i$. Notice that $C_{pq}$ and $\mathcal{O}_{U_X}^{(p)}$ are independent of indices $i, j$ due to the permutational symmetry.

To avoid confusion, we have to stress that the above covariance matrix $C = (C_{pq})$ is different from Eq. (A3) in Appendix A in general. If the spatially-separated reduced state $\varrho_{A_iB_j}$ is also permutationally symmetric, both are the same, but here we do not require the assumption.

Using the formula in Eq. (A9a) in Appendix A, we have that

$$\mathcal{G}_{AB}^{(2)}(\varrho_{AB}) = g\frac{N^4}{4^2}\sum_{p,q,r,s=x,y,z} C_{pq}C_{rs}\int dU_A \, \mathcal{O}_{U_A}^{(p)}\mathcal{O}_{U_A}^{(r)}\int dU_B \, \mathcal{O}_{U_B}^{(q)}\mathcal{O}_{U_B}^{(s)} = \sum_{p,q=x,y,z} C_{pq}^2, \tag{D8}$$

where we set that $g = (3/N^2)^2$. Also, since $\langle J_{z,A}\rangle_{U_A} = (N/4)\sum_{p=x,y,z} a_p \mathcal{O}_{U_A}^{(p)}$ and $\beta = 12/N^2$, we can find

$$\mathcal{J}_A^{(1)}(\varrho_A) = \beta\frac{N^2}{4^2}\sum_{p,q=x,y,z} a_p a_q \int dU_A\, \mathcal{O}_{U_A}^{(p)}\mathcal{O}_{U_A}^{(q)} = \sum_{p=x,y,z} a_p^2, \tag{D9}$$

as well as $\mathcal{J}_B^{(1)}(\varrho_B) = \sum_{p=x,y,z} b_p^2$. In summary, for the choice $g = (3/N^2)^2$ and $(\alpha,\beta,\gamma) = (0, 12/N^2, 0)$, we have that

$$\mathcal{G}_{AB}^{(2)} + \mathcal{J}_A^{(1)} + \mathcal{J}_B^{(1)} - \mathcal{J}_A^{(1)}\mathcal{J}_B^{(1)} = \sum_{p,q=x,y,z} C_{pq}^2 + \sum_{p=x,y,z}(a_p^2 + b_p^2) - \sum_{p,q=x,y,z} a_p^2 b_q^2. \tag{D10}$$

To derive the entanglement criterion, we rewrite the right-hand-side in Eq. (D10) as

$$\mathcal{G}_{AB}^{(2)} + \mathcal{J}_A^{(1)} + \mathcal{J}_B^{(1)} - \mathcal{J}_A^{(1)}\mathcal{J}_B^{(1)} = \sum_{p,q=x,y,z}(t_{pq}^2 - 2a_p b_q t_{pq}) + \sum_{p=x,y,z}(a_p^2 + b_p^2), \tag{D11}$$

where we use that $C_{pq}^2 = t_{pq}^2 + a_p^2 b_q^2 - 2a_p b_q t_{pq}$. To proceed further, we recall the separability criterion presented in Ref. [16] (see, Proposition 5): if a bipartite quantum state $\varrho_{XY}$ is separable, then it obeys that

$$\mathrm{tr}(\varrho_{XY}^2) + \mathrm{tr}(\varrho_X^2) + \mathrm{tr}(\varrho_Y^2) - 2\mathrm{tr}[\varrho_{XY}(\varrho_X\otimes\varrho_Y)] \leq 1. \tag{D12}$$

If $\varrho_{XY}$ is a two-qubit state, we can rewrite this inequality as

$$\sum_{i,j=x,y,z}(z_{ij}^2 - 2x_i y_j z_{ij}) + \sum_{i=x,y,z}(x_i^2 + y_i^2) \leq 1, \tag{D13}$$

where $x_i = \mathrm{tr}(\varrho_X\sigma_i)$, $y_i = \mathrm{tr}(\varrho_Y\sigma_i)$, and $z_{ij} = \mathrm{tr}(\varrho_{XY}\sigma_i\otimes\sigma_j)$. Let us apply this criterion to Eq. (D11). Exchanging the symbols

$$x_i \longleftrightarrow a_p, \quad y_i \longleftrightarrow b_p \quad z_{ij} \longleftrightarrow t_{pq}, \tag{D14}$$

we can connect this criterion to Eq. (D11) and arrive at the inequality in Observation 4. Hence we can complete the proof. □

**Remark D1.** The right-hand-side in Eq. (D10), that is, the right-hand-side in Eq. (17) in Observation 4 in the main text, can be rewritten as

$$\mathcal{G}_{AB}^{(2)} + \mathcal{J}_A^{(1)} + \mathcal{J}_B^{(1)} - \mathcal{J}_A^{(1)}\mathcal{J}_B^{(1)} = \frac{1}{N^4}\left\{\sum_{p,q}\eta_{pq}^2 + 4N^2\sum_p\left[\langle J_{p,A}\rangle^2 + \langle J_{p,B}\rangle^2\right] - 16\sum_{p,q}\langle J_{p,A}\rangle^2\langle J_{q,B}\rangle^2\right\}, \tag{D15}$$

where

$$\sum_{p=x,y,z} a_p^2 = \left(\frac{2}{N}\right)^2\sum_{p=x,y,z}\langle J_{p,A}\rangle^2, \tag{D16a}$$

$$\sum_{p=x,y,z} b_p^2 = \left(\frac{2}{N}\right)^2\sum_{p=x,y,z}\langle J_{p,B}\rangle^2, \tag{D16b}$$

$$\sum_{p,q=x,y,z} C_{pq}^2 = \left(\frac{1}{N^2}\right)^2\sum_{p,q=x,y,z}\left[(\Delta J_p^+)^2 - (\Delta J_q^-)^2\right]^2 \equiv \left(\frac{1}{N^2}\right)^2\sum_{p,q=x,y,z}\eta_{pq}^2, \tag{D16c}$$

and $\eta_{pq} \equiv (\Delta J_p^+)^2 - (\Delta J_q^-)^2$.

**Remark D2.** Here we consider the generalization of Observation 4 in the main text to $m$ ensembles for $m \geq 3$. For that, let us define a quantum state $\varrho \in \mathcal{H}_1\otimes\cdots\otimes\mathcal{H}_m$, where $\mathcal{H}_X = \mathcal{H}_2^{\otimes N}$ for $X = 1,\ldots,m$. Now it is essential to notice that the left-hand-side in Observation 4 can be available for any two-pair in $m$ ensembles. Then, let us define the average over all pairs

$$\mathcal{P}(\varrho) = \frac{2}{m(m-1)}\sum_{X<Y}\mathcal{G}_{XY}^{(2)} + \mathcal{J}_X^{(1)} + \mathcal{J}_Y^{(1)} - \mathcal{J}_X^{(1)}\mathcal{J}_Y^{(1)}, \tag{D17}$$

for $X, Y = 1, 2, \ldots, m$. Now we can formulate the following.

**Remark D3.** *For this $mN$-qubit state $\varrho$ consisting of the $m$ ensembles of $N$ spin-$\frac{1}{2}$ particles, if each $N$-qubit ensemble is permutationally symmetric, then any fully separable $\varrho$ obeys*

$$\mathcal{P}(\varrho) \leq 1, \tag{D18}$$

*where $g = (3/N^2)^2$ and $(\alpha, \beta, \gamma) = (0, 12/N^2, 0)$.*

*Proof.* In general, if a multipartite state $\varrho$ is fully separable, then all the bipartite reduced states are clearly separable. For such separable reduced states, Observation 4 in the main text holds. Thus we can complete the proof. □

**Remark D4.** Let us test our criterion in Observation 4 in the main text with the Dicke state as a bipartite state. The $N_{AB}$-qubit Dicke state with $m_{AB}$ excitations is defined as

$$|N_{AB}, m_{AB}\rangle = \binom{N_{AB}}{m_{AB}}^{-\frac{1}{2}} \sum_{m_{AB}} \mathcal{P}_{m_{AB}}(|1_1, \ldots, 1_{m_{AB}}, 0_{m_{AB}+1}, \ldots, 0_{N_{AB}}\rangle), \tag{D19}$$

where $\{\mathcal{P}_{m_{AB}}\}$ is the set of all distinct permutations in the qubits. Applying the Schmidt decomposition to the Dicke state, one can have

$$|N_{AB}, m_{AB}\rangle = \sum_{m=0}^{N_{AB}} \lambda_m \, |N_A, m_A\rangle \otimes |N_B, m_B\rangle \,, \tag{D20}$$

where $N_A + N_B = N_{AB}$, $m_A + m_B = m_{AB}$, and $m = m_A$. Here, the Schmidt coefficients $\lambda_m$ are given by

$$\lambda_m = \binom{N_{AB}}{m_{AB}}^{-\frac{1}{2}} \binom{N_A}{m_A}^{\frac{1}{2}} \binom{N_B}{m_B}^{\frac{1}{2}}. \tag{D21}$$

The states $|N_A, m_A\rangle$ and $|N_B, m_B\rangle$ are permutationally symmetric states, for details, see [56, 119].

Let us consider the case where $N_A = N_B = N_{AB}/2$, and $m_{AB} = N_{AB}/2$. Then we have

$$\langle J_{p,A}\rangle = \langle J_{p,B}\rangle = 0, \quad \text{for} \quad p = x, y, z, \tag{D22a}$$

$$\langle J_z^2\rangle = (\Delta J_z^+)^2 = 0, \tag{D22b}$$

$$(\Delta J_z^-)^2 = -4\langle J_{z,A} \otimes J_{z,B}\rangle = \frac{N_{AB}^2}{4(N_{AB}-1)}, \tag{D22c}$$

$$(\Delta J_x^+)^2 = (\Delta J_y^+)^2 = \frac{N_{AB}}{4}\left(\frac{N_{AB}}{2} + 1\right), \tag{D22d}$$

$$(\Delta J_x^-)^2 = (\Delta J_y^-)^2 = \frac{N_{AB}}{8}\frac{N_{AB}-2}{N_{AB}-1}, \tag{D22e}$$

where we used the results in Ref. [99]. Then we have the values of $(\Delta J_p^{\pm})^2$. In this paper, we set $N_{AB} = 2N$. This results in

$$\mathcal{G}_{AB}^{(2)} + \mathcal{J}_A^{(1)} + \mathcal{J}_B^{(1)} - \mathcal{J}_A^{(1)}\mathcal{J}_B^{(1)} = \frac{1}{N^4} \sum_{p,q=x,y,z} \left[(\Delta J_p^+)^2 - (\Delta J_q^-)^2\right]^2 = \frac{6N^4 - 2N^3 + 1}{(1-2N)^2 N^2}. \tag{D23}$$

The right-hand side monotonically decreases as $N$ increases, and it becomes $3/2$ when $N \to \infty$. Therefore the pure $2N$-qubit Dicke states can be detected in any $N$.

Finally, let us consider the case where the global depolarizing channel with noise $p$ influences the state as follows: $\varrho_D \to \varrho_D' = p\varrho_D + (1-p)\varrho_{\rm mm}$ for $\varrho_D = |N_{AB}, m_{AB}\rangle\langle N_{AB}, m_{AB}|$ and the maximally mixed state $\varrho_{\rm mm}$. This noise

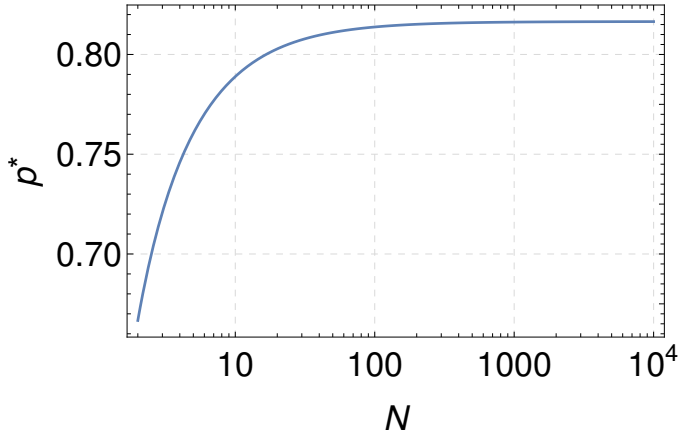


Figure 5. Linear-Log plot of the critical point $p^*(N)$ discussed in Remark D4.

effects can change $(\Delta J_l^{\pm})^2$ as follows:

$$(\Delta J^+_{x/y})^2_{\varrho_D} \to (\Delta J^+_{x/y})^2_{\varrho'_D} = \frac{N_{AB}}{4} + p\left[(\Delta J^+_{x/y})^2_{\varrho_D} - \frac{N_{AB}}{4}\right] = \frac{N(1+Np)}{2}, \tag{D24a}$$

$$(\Delta J^-_{x/y})^2_{\varrho_D} \to (\Delta J^-_{x/y})^2_{\varrho'_D} = \frac{N_{AB}}{4} + p\left[(\Delta J^-_{x/y})^2_{\varrho_D} - \frac{N_{AB}}{4}\right] = \frac{N[N(2-p)-1]}{2(2N-1)}, \tag{D24b}$$

$$(\Delta J^+_{z})^2_{\varrho_D} \to (\Delta J^+_{z})^2_{\varrho'_D} = \frac{N_{AB}(1-p)}{4} = \frac{N(1-p)}{2}, \tag{D24c}$$

$$(\Delta J^-_{z})^2_{\varrho_D} \to (\Delta J^-_{z})^2_{\varrho'_D} = \frac{N_{AB}}{4} + p\left[(\Delta J^-_{z})^2_{\varrho_D} - \frac{N_{AB}}{4}\right] = \frac{N(2N+p-1)}{2(2N-1)}. \tag{D24d}$$

This leads to

$$\mathcal{G}^{(2)}_{AB} + \mathcal{J}^{(1)}_A + \mathcal{J}^{(1)}_B - \mathcal{J}^{(1)}_A \mathcal{J}^{(1)}_B = \frac{\left(6N^4 - 2N^3 + 1\right)p^2}{(1-2N)^2 N^2}. \tag{D25}$$

Then we can find that the separability bound in Observation 4 is violated when $p > p^*(N)$ for the critical point

$$p^*(N) = \frac{N(2N-1)}{\sqrt{6N^4 - 2N^3 + 1}}. \tag{D26}$$

In Fig. 5, we illustrate the behavior of the critical point depending on $N$. In the limit $N \to \infty$, this point becomes $p^* \to \sqrt{2/3}$.

## Appendix E: Entanglement detection with finite statistics

In Appendix E, we will discuss the estimation of the statistical error of the moments from collective randomized measurements. We will determine the number of measurements required for reliable entanglement detection, following similar discussions given in the previous works [2, 8–10, 15].

In randomized measurement schemes, the total number of measurements is denoted as $M_{\text{tot}} = M \times K$. Here $M$ is the number of random unitaries, and $K$ is the number of measurements for a fixed unitary. For the moment $\mathcal{J}^{(r)} = \int dU\, [f_U]^r$ defined in Eq. (4) in the main text, the unbiased estimator can be given by $\tilde{\mathcal{J}}^{(r)} = (1/M)\sum_{i=1}^{M}[\tilde{f}_r]_i$, that is, $\mathbb{E}_U\mathbb{E}[\tilde{\mathcal{J}}^{(r)}] = \mathcal{J}^{(r)}$. Here, the subscript $i$ in $[\tilde{f}_r]_i$ refers to the measurement setting, $\mathbb{E}_U$ represents the average over collective local random unitaries, and $\tilde{f}_r$ is the unbiased estimator of $[f_U]^r$, that is, $\mathbb{E}[\tilde{f}_r] = [f_U]^r$.

To quantify how much the estimator $\tilde{\mathcal{J}}^{(r)}$ deviates from the $\mathcal{J}^{(r)}$, let us consider the inequality

$$\text{Prob}(\tilde{\mathcal{J}}^{(r)} - \mathcal{J}^{(r)} \geq \delta_{\text{error}}) \leq \alpha_{\text{ssl}}, \tag{E1}$$

where $\delta_{\rm error}$ is called the error or accuracy, $\alpha_{\rm ssl}$ the statistical significance level, and $\gamma_{\rm cl} = 1 - \alpha_{\rm ssl}$ the confidence level. In the case where $[\tilde{f}_r]_i$ cannot be assumed to be i.i.d. random variables, we can employ the so-called (one-sided) Chebyshev-Cantelli inequality

$$\mathrm{Prob}\left(\tilde{\mathcal{J}}^{(r)} - \mathcal{J}^{(r)} \geq \delta_{\rm error}\right) \leq \frac{\mathrm{Var}(\tilde{\mathcal{J}}^{(r)})}{\mathrm{Var}(\tilde{\mathcal{J}}^{(r)}) + \delta^2_{\rm error}}, \tag{E2}$$

where $\mathrm{Var}(\tilde{\mathcal{J}}^{(r)})$ denotes the variance of the estimator $\tilde{\mathcal{J}}^{(r)}$. Based on this inequality, one can determine the total number of measurements $M_{\rm tot} = M \times K$ required for entanglement detection, for a fixed error and confidence level. Since it holds that $\mathrm{Var}(\tilde{\mathcal{J}}^{(r)}) = (1/M^2)\sum_{i=1}^{M} \mathrm{Var}([\tilde{f}_r]_i)$, the main task is to evaluate the variance $\mathrm{Var}([\tilde{f}_r]_i)$.

In the following, as a simple example, we will particularly focus on Observation 2 in the main text: the moment $\mathcal{J}^{(1)} = \int dU\, [3(\Delta J_z)^2_U]$ is equal to $\sum_{l=x,y,z}(\Delta J_l)^2$, and any $N$-qubit fully separable state obeys $\mathcal{J}^{(1)}(\varrho) \geq N/2$. Now the variance is written as $\mathrm{Var}(\tilde{f}_1) = \mathbb{E}_U\mathbb{E}[(\tilde{f}_1)^2] - [\mathcal{J}^{(1)}]^2$, and the explicit form of $\mathbb{E}[(\tilde{f}_1)^2]$ can be given by

$$\mathbb{E}[(\tilde{f}_1)^2] = 9\left\{c_1(K)\langle J_z^4\rangle_U + c_2(K)\langle J_z^3\rangle_U\langle J_z\rangle_U + c_3(K)\langle J_z^2\rangle_U^2 + c_4(K)\langle J_z^2\rangle_U\langle J_z\rangle_U^2 + c_5(K)\langle J_z\rangle_U^4\right\}, \tag{E3}$$

where $c_1(K) = 1/K$, $c_2(K) = -4/K$, $c_3(K) = [(K-1)^2+2]/[K(K-1)]$, $c_4(K) = -2(K-2)(K-3)/[K(K-1)]$, and $c_5(K) = (K-2)(K-3)/[K(K-1)]$. This expression can be derived using the result in Ref. [120] that coincides with [121].

Let us consider the statistically significant test with the family of the states

$$\varrho_p = (1-p)\varrho_{\rm singlet} + p\frac{\mathbb{1}}{2^N}, \tag{E4}$$

where $\varrho_{\rm singlet}$ denotes the $N$-qubit many-body spin singlet state, discussed in the main text. Since this state obeys $\langle J_l^k\rangle_{\varrho_{\rm singlet}} = 0$ for any $k$, we have that $\langle J_l\rangle_{\varrho_p} = 0$, $\langle J_l^2\rangle_{\varrho_p} = Np/4$, and therefore, $\mathcal{J}^{(1)}(\varrho_p) = 3Np/4$. Thus, the state $\varrho_p$ violates the separability bound in Observation 2 when $p$ becomes smaller than the critical point $p_{\rm sep} = 2/3$, which is independent of $N$. From a straightforward calculation, we can obtain

$$\mathrm{Var}(\tilde{\mathcal{J}}^{(1)}) = \frac{9Np\{3N(p-1)+2-K[N(p-3)+2]\}}{[16(K-1)K]M}, \tag{E5}$$

where we used $\langle J_l^4\rangle_{\varrho_p} = N(3N-2)p/16$. Rearranging the Chebyshev-Cantelli inequality in Eq. (E2) and requiring that the confidence $1 - \mathrm{Prob}(\tilde{\mathcal{J}}^{(1)} - \mathcal{J}^{(1)} \geq \delta_{\rm error})$ is at least $\gamma_{cl}$, we have

$$\delta_{\rm error} = \sqrt{\frac{\gamma_{\rm cl}}{1-\gamma_{\rm cl}}\mathrm{Var}(\tilde{\mathcal{J}}^{(1)})}. \tag{E6}$$

Since the variance $\mathrm{Var}(\tilde{\mathcal{J}}^{(1)})$ can monotonically increase for large $p$, the worst-case error in the estimation is given by $p = 1$. In this case, we have

$$M = \frac{9\gamma_{\rm cl}N[K(N-1)+1]}{8(1-\gamma_{\rm cl})(K-1)K\delta^2_{\rm error}}. \tag{E7}$$

To proceed, let us set the error as $\delta_{\rm error} = \min_{\varrho_{\rm sep}\in{\rm SEP}}\mathcal{J}^{(1)}(\varrho_{\rm sep}) - \mathcal{J}^{(1)}(\varrho_p) = N/2 - 3Np/4$. By minimizing the value of $M_{\rm tot} = M(K) \times K$ with respect to $K$ for a fixed $N$, we can thus find the optimal number of measurements. In Fig. 6, we illustrate the necessary number of measurements for $N = 100$ and the confidence level $\gamma_{\rm cl} = 0.95$.

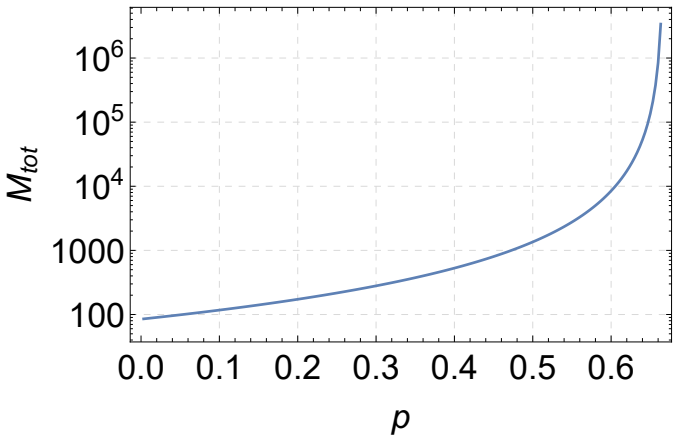


Figure 6. Log plot of the total number of measurements $M_{\text{tot}}$ obtained from the Chebyshev-Cantelli inequality required to certify the violation of the separability bound in Observation 2 in the main text of $\varrho_p$, for $N = 10^2$ and confidence level $\gamma_{\text{cl}} = 0.95$.