

<https://doi.org/10.1038/s41534-025-00990-6>

High-dimensional entanglement witnessed by correlations in arbitrary bases

Nicky Kai Hong Li^{1,2,3}✉, Marcus Huber^{1,3} & Nicolai Friis^{1,3}

Certifying entanglement is an important step in the development of many quantum technologies, especially for higher-dimensional systems, where entanglement promises increased capabilities for quantum communication and computation. A key feature distinguishing entanglement from classical correlations is the occurrence of correlations for complementary measurement bases. In particular, mutually unbiased bases (MUBs) are a paradigmatic example that is well-understood and routinely employed for entanglement certification. However, implementing unbiased measurements exactly is challenging and not generically possible for all physical platforms. Here, we extend the entanglement-certification toolbox from correlations in MUBs to arbitrary bases. This practically significant simplification paves the way for efficient characterizations of high-dimensional entanglement in a wide range of physical systems. Furthermore, we introduce a simple three-MUBs construction for all dimensions without using the Wootters–Fields construction, potentially simplifying experimental requirements when measurements in more than two MUBs are needed, especially in high-dimensional settings.

Entanglement is an important signature of “quantumness” and a central resource in quantum information processing. In particular, it is a crucial ingredient to achieving quantum advantages in many communication^{1–5}, metrological^{6,7}, and computational tasks⁸. Consequently, continuous efforts are being made to develop mathematical tools for the detection and quantification of entanglement in experiments⁹.

The certification of high-dimensional entanglement is of particular relevance to setups that use multilevel quantum systems to store and process information^{10,11}. Entanglement in higher dimensions can be more robust to noise and can allow for higher data throughput when used for teleportation, such that the performance of many quantum information-processing tasks improves with the dimension of the accessible entanglement resources. For example, using higher-dimensional entanglement can improve secure key rates in quantum key distribution¹² and benefit a wide range of quantum technologies such as entanglement-enhanced imaging^{13–15}.

Moreover, entanglement certification can serve as a benchmark for quantum computers and simulators: If a device is supposed to output states with high-dimensional entanglement, then certifying the latter in the actual outputs can indicate how well the device is functioning^{11,16}. At the same time, entanglement certification can increase one’s confidence that a quantum advantage can be achieved since the hardness of

classically simulating a many-body system increases with the amount of entanglement^{17–19}.

A central intuition behind entanglement detection is that entanglement leads to correlations between outcomes of local measurements in two or more complementary bases. In this context, complementarity is typically approached via the extremal case of mutually unbiased bases (MUBs). For a quantum system prepared in any basis state of any one of these bases, all measurement outcomes for any of the other MUBs are equally likely, i.e., knowing the measurement outcome in one basis tells us nothing about the outcomes in the complementary bases. Consequently, MUBs have been at the centre of many existing entanglement-detection methods^{10,20–23}. Correlations measured in MUBs can in turn be used to bound well-defined figures of merit that quantify how strongly entangled the underlying state is. An example of such a quantity is the Schmidt number²⁴—a generalization of the Schmidt rank for mixed states—that is used here to quantify entanglement dimensionality.

However, while some systems allow one to freely select the measurement bases (e.g., via spatial light modulators and single-mode fibres for spatial degrees-of-freedom of photons^{10,22}), this is generically not the case for all setups. The inability to measure in the desired MUBs often goes hand in hand with (but does not mathematically imply) the impossibility of carrying

¹Atominstut, Technische Universität Wien, Stadionallee 2, 1020 Vienna, Austria. ²Vienna Center for Quantum Science and Technology, TU Wien, 1020 Vienna, Austria. ³Institute for Quantum Optics and Quantum Information (IQOQI), Austrian Academy of Sciences, Boltzmanngasse 3, 1090 Vienna, Austria.

✉ e-mail: kai.li@tuwien.ac.at

out tomographically complete sets of measurements. For previous approaches to certifying high-dimensional entanglement, such limited control has been prohibitively restrictive.

Nevertheless, classical correlations cannot simultaneously be arbitrarily strong for any set of bases that are complementary in the sense of corresponding to non-commuting observables. Indeed, the detection of bipartite entanglement from measurements in arbitrary bases can, in principle, be achieved via entropic uncertainty relations^{25,26}, which provide a lower bound on the entanglement cost²⁷, but not on the Schmidt number.

In this work, we fill this gap by proposing a family of Schmidt-number witnesses based on correlations in at least two coordinated local orthonormal bases which can be chosen arbitrarily. We provide analytic upper bounds of the corresponding witness operators evaluated on any bipartite state with Schmidt number at most k (Theorem 1 & Lemma 1). The main advantage of our method is that the upper bounds depend only on the absolute values of the basis-vector overlaps and are independent of the relative phases between the measurement bases, which are often not directly measurable in experiments. Therefore, our witness significantly simplifies the requirements for certifying high-dimensional entanglement in experiments across a wider range of platforms. We also show that the bounds are the tightest when the underlying measurement bases are mutually unbiased (Corollary 1), confirming the intuition that MUBs are optimal for entanglement detection within this framework.

In addition, we analytically lower bound the *entanglement fidelity* (or the *singlet fraction*^{28,29})—the maximum fidelity of a bipartite state with any two-qudit maximally entangled state—using our witness (Theorem 1 & Lemma 1). This provides an alternative way to quantify high-dimensional entanglement. Next, we demonstrate the effectiveness of our Schmidt-number witnesses with two examples: the two-qudit isotropic state and the noisy two-qudit purified thermal states, and evaluate the difference between the actual entanglement fidelity and our bound for these examples (see also the Supplementary Information which includes the detailed analyses of the examples of isotropic states and noisy purified thermal states, discussions regarding the applications of random measurement bases and AMUBs, the proofs of eqs. (12) and (13) and Lemma 2, and refs. 30–47). To complete our analysis, we compare the white-noise tolerances of our witnesses with those proposed in ref. 10. We also discuss the possibility of using random measurement bases in high dimensions or approximately MUBs (AMUBs) (see the Supplementary Information) to witness Schmidt numbers and propose a simple (and, to the best of our knowledge, new) construction of three MUBs for all dimensions without using the Wootters-Fields construction⁴⁸. Finally, we compare various existing methods for certifying high-dimensional entanglement with our method in Table 1.

Results

Background and notation

To detect bipartite entanglement, parties A and B measure their shared state ρ_{AB} in m local bases with global projectors $|e_a^z\rangle\langle e_a^z| \otimes |\tilde{e}_a^{z*}\rangle\langle \tilde{e}_a^{z*}|$ where $\{|e_a^z\rangle\}_{a=0}^{d-1}$ is the z -th orthonormal basis of the m bases, $|\phi^*\rangle$ denotes the complex conjugate of the state $|\phi\rangle$ with respect to the computational basis $\{|i\rangle\}_{i=0}^{d-1}$, and $|\tilde{e}_a^{z*}\rangle := U|e_a^{z*}\rangle$ with $U \in U(d)$ fixed for all a and z . Note that we do not require the m measurement bases to be MUBs as in ref. 23. The entanglement witness is then defined to be the sum of the probabilities of all matching outcomes in all matching pairs of bases, i.e.,

$$S_d^{(m)}(\rho_{AB}) = \sum_{z=1}^m \sum_{a=0}^{d-1} \langle e_a^z, \tilde{e}_a^{z*} | \rho_{AB} | e_a^z, \tilde{e}_a^{z*} \rangle. \quad (1)$$

In Theorem 1, we show how the upper bound of eq. (1) depends on the Schmidt number $k(\rho_{AB})$ ²⁴ of the state ρ_{AB} , which is defined as

$$k(\rho_{AB}) := \inf_{\mathcal{D}(\rho_{AB})} \left\{ \max_{\{(p_i, |\psi_i\rangle)\}_i} \text{rank}(\text{Tr}_B |\psi_i\rangle\langle \psi_i|) \right\}, \quad (2)$$

where $\mathcal{D}(\rho)$ is the set of all pure-state decompositions, $\{(p_i, |\psi_i\rangle)\}_i$, of $\rho = \sum_i p_i |\psi_i\rangle\langle \psi_i|$ and $\{p_i\}_i$ is a probability distribution. In addition, we show that the maximum fidelity of ρ_{AB} with any maximally entangled state,

$$\mathcal{F}(\rho_{AB}) := \max_{U_A} \langle \Phi_d^+ | (U_A \otimes \mathbb{1}_B) \rho_{AB} (U_A \otimes \mathbb{1}_B)^\dagger | \Phi_d^+ \rangle, \quad (3)$$

where the maximization is over all unitaries U_A acting on subsystem A and $|\Phi_d^+\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |ii\rangle$, can be lower bounded using the quantity $S_d^{(m)}(\rho_{AB})$. From now on, we call $\mathcal{F}(\rho_{AB})$ the *entanglement fidelity* (also known as the *singlet fraction* in the case of qubits^{28,29}) of ρ_{AB} .

Let us define the maximum and minimum overlaps between two bases z and z' as $c_{\max}^{z,z'} = \max_{a,a'} |\langle e_a^z | e_{a'}^{z'} \rangle|^2$ and $c_{\min}^{z,z'} = \min_{a,a'} |\langle e_a^z | e_{a'}^{z'} \rangle|^2$, respectively. We then define $\mathcal{C} = \{|\langle e_a^z | e_{a'}^{z'} \rangle|^2\}_{a,a',z \neq z'}$ ($\bar{\mathcal{C}} = \{(c_{\max}^{z,z'}, c_{\min}^{z,z'})\}_{z \neq z'}$) to be the set that contains all (pairs of maximum and minimum) overlaps between any two different measurement bases.

Schmidt-number witness & entanglement-fidelity bound

We now present our main results that use the expectation value $S_d^{(m)}$ to infer lower bounds on the Schmidt number and entanglement fidelity of the state ρ_{AB} .

Theorem 1. For any bipartite state ρ_{AB} of equal local dimension d and Schmidt number at most k , it holds that

$$S_d^{(m)}(\rho_{AB}) \leq \frac{k(m - T(\mathcal{C}))}{d} + T(\mathcal{C}) =: \mathcal{B}_k, \quad (4)$$

where the upper bound \mathcal{B}_k depends on the integers d and k , the number of measurement bases m , and a quantity $T(\mathcal{C})$ which depends on the set of bases overlaps. More specifically, $T(\mathcal{C}) := \min\{\lambda(\mathcal{C}), m\}$, $\lambda(\mathcal{C}) := \frac{1}{2} \left(1 + \sqrt{1 + 2d \sum_{z \neq z'} G^{z,z'}} \right) \geq 1$, and $G^{z,z'} := 1 - (d+1)c_{\min}^{z,z'} + \frac{1}{d} \sum_{a,a'} |\langle e_a^z | e_{a'}^{z'} \rangle|^4$. Furthermore, the entanglement fidelity of ρ_{AB} can be lower bounded as follows:

$$\mathcal{F}(\rho_{AB}) \geq \max \left\{ 0, \frac{S_d^{(m)}(\rho_{AB}) - T(\mathcal{C})}{m - T(\mathcal{C})} \right\} =: \mathcal{F}_m. \quad (5)$$

The proof of Theorem 1 is given in full in the Methods. Theorem 1 implies that if the measured quantity $S_d^{(m)}(\rho_{AB})$ exceeds \mathcal{B}_k for $1 \leq k \leq d-1$, then the Schmidt number of ρ_{AB} must be at least $k+1$. For a given set of local measurement bases $\{ \{|e_a^z\rangle\}_{a=0}^{d-1} \}_{z=1}^m$, parties A and B can maximize the certified Schmidt number by choosing U (their relative reference frame) that maximizes $S_d^{(m)}(\rho_{AB})$ since the upper bound in eq. (4) is independent of U . Notice that if all the measurement bases are MUBs, i.e., $|\langle e_a^z | e_{a'}^{z'} \rangle|^2 = \frac{1}{d} \forall a, a', z \neq z'$, then $T(\mathcal{C}) = 1$ and the bound in eq. (4) coincides with the one in ref. 23. Since $T(\mathcal{C}) \geq 1$ for any $m \geq 2$, we immediately arrive at Corollary 1.

Corollary 1. The bound \mathcal{B}_k in eq. (4) is the tightest for all $k < d$ when the m measurement bases are MUBs.

In case we only have access to the set of maximum and minimum overlaps $\bar{\mathcal{C}}$ instead of all the overlaps \mathcal{C} , we can still bound the Schmidt number and the entanglement fidelity by loosening the bounds in Theorem 1. By maximizing the term $\sum_{a,a'} |\langle e_a^z | e_{a'}^{z'} \rangle|^4$ in eq. (4) such that the overlaps are compatible with $\bar{\mathcal{C}}$, we obtain the following lemma which is proven in the Methods.

Table 1 | A comparison of different methods for the verification of high-dimensional entanglement

Methods	Features and experimental/computational requirements
Our witness	<ul style="list-style-type: none"> Measure in at least two coordinated local (arbitrary) orthonormal bases Only need to know the (minimum and maximum) absolute values of the overlaps between the local measurement bases
Reference ¹⁰ 's witness	<ul style="list-style-type: none"> Precise control over the absolute values & the complex phases of the overlaps between different local measurement bases and within each basis Measure in the computational basis + at least one coordinated “tilted” basis
SDP witness ⁵⁵	<ul style="list-style-type: none"> Treat bases bias as imperfect implementations of measurements in MUBs Memory issue/long computational runtime for large dimensions Efficient only for small dimensions in which case it is possible to obtain tighter bounds compared to our witness
Entropic uncertainty relationship ^{25,27} [eq. (17.135) in ref. 56]	<ul style="list-style-type: none"> Need to know the absolute values of the bases overlaps of only one party and the classical entropies corresponding to the two parties' measurements Can lower bound the distillable entanglement instead of the Schmidt number
Generalized Bell inequalities ^{57,58}	<ul style="list-style-type: none"> To witness Schmidt number without any measurement assumptions, require non-trivial optimization over all possible local measurements and all states with Schmidt number $\leq k$ for every local dimension, which is computationally costly Certify lower Schmidt numbers than other methods can in general Standard approaches involve finding the largest eigenvalue corresponding to eigenvectors with Schmidt rank $\leq k$ of the Bell operator⁵⁹ associated with restricted measurement settings^{58,60} to keep optimization problems numerically tractable (more specifically, ref. 58 uses physical arguments to restrict the maximization of the Bell operator's expectation value to restricted sets of states with different maximum Schmidt numbers—referred to therein as entanglement dimensions—of which the union is believed to contain the experimental states) → also require measurement assumptions and are computationally feasible only for small dimensions
Correlation-matrix norms from randomized measurements ⁶¹	<ul style="list-style-type: none"> Independent of the relative reference frame between the two parties as the matrix p-norms for all even $p \in \mathbb{N}$ of the correlation matrix remain unchanged under any local unitary transformation of a bipartite state⁶¹. Require sampling local unitaries randomly from (Haar measure or) t-designs, where exact sampling is highly inefficient⁶². While approximate sampling from t-designs can be efficient⁶³, it is unclear how approximate sampling can affect the Schmidt-number witness in ref. 61. Analytic bounds of the 2- and 4-norms of the correlation matrices corresponding to states with Schmidt number $\leq k$ are known only for $k = 2$ For certifying Schmidt number ≥ 3, require numerical optimizations which can be computationally costly for large dimensions and the bounds can be loose since there are no tighter known constraints on the singular values of the correlation matrix other than the purity bound $\text{Tr}(\rho^2) < 1$ (see Appendix C of ref. 61.)

Lemma 1. For any bipartite state ρ_{AB} of equal local dimension d and Schmidt number at most k , it holds that

$$\mathcal{S}_d^{(m)}(\rho_{AB}) \leq \frac{k(m - \bar{\mathcal{T}}(\bar{\mathcal{C}}))}{d} + \bar{\mathcal{T}}(\bar{\mathcal{C}}) =: \bar{\mathcal{B}}_k, \quad (6)$$

where the upper bound $\bar{\mathcal{B}}_k$ depends on d, k , the number of measurement bases m , and a quantity $\bar{\mathcal{T}}(\bar{\mathcal{C}})$ which depends on the set of minimum and maximum bases overlaps. More specifically, $\bar{\mathcal{T}}(\bar{\mathcal{C}}) := \min\{\bar{\lambda}(\bar{\mathcal{C}}), m\}$,

$$\bar{\lambda}(\bar{\mathcal{C}}) := \frac{1}{2} \left(1 + \sqrt{1 + 2d \sum_{z, z'} \bar{G}(c_{\max}^{z, z'}, c_{\min}^{z, z'})} \right) \geq 1, \quad \bar{G}(c_{\max}^{z, z'}, c_{\min}^{z, z'}) := 1 - (d + 1)c_{\min}^{z, z'} + \Omega^{z, z'}, \quad \Omega^{z, z'} := L^{z, z'}(c_{\max}^{z, z'})^2 + (d - L^{z, z'} - 1)(c_{\min}^{z, z'})^2 + [1 - L^{z, z'}c_{\max}^{z, z'} - (d - L^{z, z'} - 1)c_{\min}^{z, z'}]^2, \text{ and}$$

$$L^{z, z'} := \begin{cases} \left\lfloor \frac{1 - c_{\min}^{z, z'} d}{c_{\max}^{z, z'} - c_{\min}^{z, z'}} \right\rfloor & \text{if } c_{\max}^{z, z'} > c_{\min}^{z, z'}, \\ d & \text{if } c_{\max}^{z, z'} = c_{\min}^{z, z'}. \end{cases} \quad (7)$$

Furthermore, the entanglement fidelity of ρ_{AB} can be lower bounded as follows:

$$\mathcal{F}(\rho_{AB}) \geq \max \left\{ 0, \frac{\mathcal{S}_d^{(m)}(\rho_{AB}) - \bar{\mathcal{T}}(\bar{\mathcal{C}})}{m - \bar{\mathcal{T}}(\bar{\mathcal{C}})} \right\} =: \bar{\mathcal{F}}_m. \quad (8)$$

Similar to Theorem 1, if $\mathcal{S}_d^{(m)}(\rho_{AB}) > \bar{\mathcal{B}}_k$, the Schmidt number of ρ_{AB} must be at least $k + 1$. Furthermore, if all the measurement bases are MUBs, i.e., $c_{\max}^{z, z'} = c_{\min}^{z, z'} = \frac{1}{d} \forall z, z'$, then $\bar{\mathcal{T}}(\bar{\mathcal{C}}) = 1$ and $\bar{\mathcal{B}}_k$ coincides with the bound in ref. 23. Since $\bar{\mathcal{T}}(\bar{\mathcal{C}}) \geq 1$, MUBs give the tightest bounds $\bar{\mathcal{B}}_k$.

Examples of witness violation

To illustrate that our method can verify Schmidt numbers and lower bound the entanglement fidelity, we first apply our witness and the fidelity bound to

a standard benchmark for entanglement witnesses, i.e., isotropic states $\rho_{AB}^{\text{iso}} = (1 - p)|\Phi_d^+\rangle\langle\Phi_d^+| + \frac{p}{d^2} \mathbb{1}_{d^2}$, whose Schmidt number is $k + 1$ if and only if the white-noise ratio p satisfies $\frac{d(d-k-1)}{d^2-1} \leq p < \frac{d(d-k)}{d^2-1} =: p_{\text{iso}}^{(k)}$ ²⁴. We compare this with the noise that our witness can tolerate until we can no longer witness the actual Schmidt number of ρ_{AB}^{iso} . Since

$$\mathcal{S}_d^{(m)}(\rho_{AB}^{\text{iso}}) = p \frac{m}{d} + (1 - p)m, \quad (9)$$

for $\mathcal{S}_d^{(m)}(\rho_{AB}^{\text{iso}})$ to exceed the bound $\bar{\mathcal{B}}_k$ in Theorem 1, the white-noise ratio must satisfy

$$p < \frac{(m - \mathcal{T}(\mathcal{C}))(d - k)}{m(d - 1)} =: p_{c, m}^{(k)}. \quad (10)$$

In the case when $d + 1$ MUBs exist and $m = d + 1$, we see that $p_{c, m}^{(k)} = p_{\text{iso}}^{(k)}$ for all k .

Suppose that we have the worst possible choice of measurement bases for a given $c_{\min} := \min_{z, z'} c_{\min}^{z, z'}$ such that $c_{\min} = c_{\min}^{z, z'}$ and $c_{\max}^{z, z'} = 1 - (d - 1)c_{\min} =: c_{\max}$ for all z, z' (As it is harder to witness a state to have Schmidt number $k + 1$ with a larger bound $\bar{\mathcal{B}}_k$, this is the worst-case bases choice for a given $c_{\min} = \min_{z, z'} c_{\min}^{z, z'}$ because (i) it gives the maximal value allowed for $c_{\max} = \max_{z, z'} c_{\max}^{z, z'}$ such that $\sum_a |(e_a^z | e_a^{z'})|^2 = 1$ holds for all a , and (ii) $\mathcal{T}(\mathcal{C})$ (and therefore $\bar{\mathcal{B}}_k$) increases with c_{\max} for a fixed c_{\min} due to the enlargement of the feasible set of the optimization problem in Proposition 3). We can use the upper bound in Lemma 1 by replacing $\mathcal{T}(\mathcal{C})$ in eq. (10) with $\bar{\mathcal{T}}(\bar{\mathcal{C}})$, where $\bar{\lambda}(\bar{\mathcal{C}}) = \frac{1}{2} (1 + \sqrt{1 + 2dm(m - 1)\bar{G}(c_{\max}, c_{\min})})$ in eq. (6). To verify that our state has Schmidt number at least $k + 1$, the bound $\bar{\mathcal{B}}_k$ must be violated. In Fig. 1, the white-noise thresholds $p_{c, m}^{(k)}$ for witnessing the Schmidt number of ρ_{AB}^{iso} in $d = 5$ to be at least $k + 1$ with m measurement bases are plotted against the parameter $\epsilon_{\min} := \frac{1}{d} - c_{\min}$,

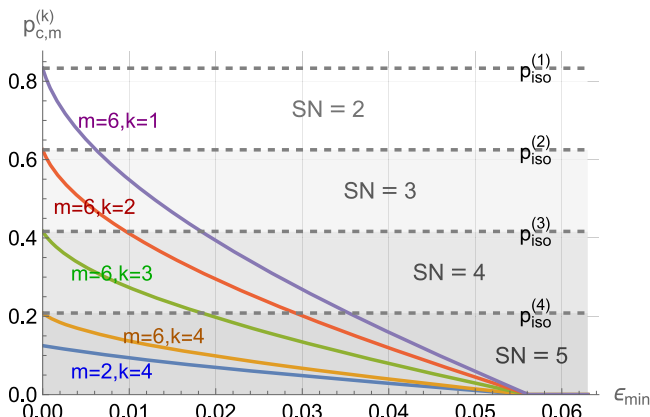


Fig. 1 | White-noise tolerance of our Schmidt-number witness. The upper bounds of the white-noise ratio, $p_{c,m}^{(k)}$ in eq. (10), for witnessing Schmidt number $k+1$ versus $\epsilon_{\min} := 1/d - c_{\min}$ in local dimension $d=5$, where we set $c_{\max} = 1 - (d-1)c_{\min}$. When $\epsilon_{\min} = 0$ (i.e., $c_{\min} = 1/d$ for MUBs), $p_{c,m}^{(k)}$ reaches its maximum, $(m-1)(d-k)/[m(d-1)]$. When $m = d+1 = 6$, it coincides with $p_{\text{iso}}^{(k)}$, the maximum white-noise ratio for ρ_{AB}^{iso} having Schmidt number $k+1$. The noise tolerance of the witness is higher for larger m or smaller k but reduces as ϵ_{\min} increases, and eventually, when $\epsilon_{\min} \geq 1/5 - (7 - \sqrt{17})/20 \approx 0.0562$, we cannot witness non-trivial Schmidt numbers of ρ_{AB}^{iso} .

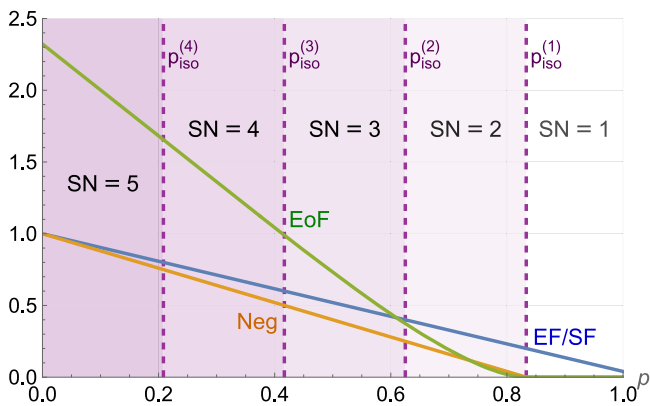


Fig. 2 | Comparing other standard measures of bipartite entanglement with the Schmidt number. The entanglement of formation (EoF), the entanglement fidelity/singlet fraction (EF/SF), the negativity (Neg), and the exact Schmidt number (SN) of the isotropic state ρ_{AB}^{iso} of $d=5$ are plotted for different white-noise ratios p .

which quantifies the deviation of the measurement bases from MUBs. Note that the maximum value that c_{\min} can take is $\frac{1}{d}$ in order for $\sum_{a'} |\langle e_a^z | e_{a'}^{z'} \rangle|^2 = 1$ to hold for all a, z and z' , so $\epsilon_{\min} \in [0, \frac{1}{d}]$. When $\epsilon_{\min} = 0$, corresponding to measurements in MUBs, $p_{c,m}^{(k)}$ attains its maximum. In general, the witness can be violated under more white noise for smaller k . In addition, as $p_{c,m}^{(k)}$ goes to zero when $\bar{\lambda}(\bar{C}) = m$, we see that whenever

$$c_{\min} \leq \frac{3d-1-\sqrt{d^2+10d-7}}{2d(d-1)}, \quad (11)$$

we cannot witness any Schmidt number $2 \leq k+1 \leq d$ of the state ρ_{AB}^{iso} as $p_{c,m}^{(k)} = 0$ for all $m \geq 2$. To see how the Schmidt number is related to other standard measures of bipartite entanglement, we also compare the entanglement of formation (EoF) (see eq. (4.2) of ref. 49), the entanglement fidelity/singlet fraction (EF/SF), and the negativity (see eq. (26) of ref. 50) with the exact Schmidt number (SN) of the isotropic state of $d=5$ for different white-noise ratios p in Fig. 2.

In the Supplementary Information, we provide more elaborate analyses of our witness when applied to isotropic states. First, we show that the

entanglement fidelity of ρ_{AB}^{iso} satisfies eq. (5) in Theorem 1. Then, we provide an example suggesting that our Schmidt-number witness can tolerate less bases bias in larger local dimensions. Finally, we compare the white-noise tolerance of our witness and our lower bound on the entanglement fidelity with the counterparts from ref. 10.

To give a more comprehensive picture, we provide another example, i.e., the purified thermal states with white noise, in the Supplementary Information, to demonstrate that our method also works in cases where the eigenvalues of the single-party reduced states are not degenerate and to compare the white-noise tolerance of our witness with that of ref. 10 in such cases. We also show that adding a third basis that is slightly biased with respect to two mutually unbiased measurement bases can increase our witness' tolerance to white noise in this example. On the other hand, adding a basis that is too biased with respect to the other bases could worsen our witnesses' performance due to an increased upper bound \mathcal{B}_k ($\bar{\mathcal{B}}_k$) in Theorem 1 (Lemma 1). We summarize this observation in the following remark.

Remark 1. There exist scenarios where an additional measurement basis improves the noise tolerance of our Schmidt-number witness. However, the opposite can also occur for certain choices of bases. Therefore, in order to witness the highest Schmidt number of a state, one should apply the witness inequality in Theorem 1 or Lemma 1 to all subsets of the total set of m' available measurement bases and find the largest k such that $\mathcal{S}_d^{(m)}(\rho) > \mathcal{B}_k$ or $\bar{\mathcal{B}}_k$ when evaluated over all subsets of m chosen bases for all $m \in \{2, \dots, m'\}$.

The intuition behind Remark 1 is that one can potentially certify a higher Schmidt number by post-selecting a subset of the total measurement data that achieves the optimal balance between showing the strongest measurement correlations and minimizing bias in the measurement bases. In practice, this can be realized easily by using as many local orthogonal measurement bases as possible for both parties and then calculating both the sum of expectation values $\mathcal{S}_d^{(m)}(\rho)$ and the bounds \mathcal{B}_k or $\bar{\mathcal{B}}_k$ for each subset of measurement bases, using the corresponding subset of the full measurement data.

As a further remark, we observe that in $d=6$, adding a fourth basis to a set with three MUBs decreases the noise tolerance for witnessing Schmidt numbers in isotropic states for a wide range of choices for the additional basis. Since it is widely believed that the maximum number of MUBs in $d=6$ is 3³⁸, this observation could indicate that our witness performs best when the local measurement bases consist only of the maximal set of MUBs in the given local dimension and no other bases.

Implication of concentration of measure

We have seen from Corollary 1 that measuring in MUBs will give the best Schmidt-number witness. However, requiring all local measurement bases to be MUBs is experimentally demanding as it requires precise control over the relative phases among all measurement bases. In light of this practical difficulty, it is natural to ask, how likely will a set of measurement bases chosen uniformly at random in \mathbb{C}^d be close to being mutually unbiased? Using Lévy's lemma^{34–36}, a result from concentration of measure, we show that the likelihood of any two randomly chosen orthonormal bases to be biased decreases exponentially with the dimension d , i.e., for $\epsilon > 0$,

$$\Pr \left\{ \left| |\langle e_a^z | e_{a'}^{z'} \rangle|^2 - \frac{1}{d} \right| > \epsilon \right\} \leq 2 \exp \left(- \frac{d\epsilon^2}{18\pi^3 \ln 2} \right), \quad (12)$$

for all a, a' and $z \neq z'$. Therefore, in large dimensions d , random measurement bases are likely to be sufficient for our method to witness high-dimensional entanglement. The proof of eq. (12) can be found in Sec. S.III of the Supplementary Information.

Maximal number of orthonormal bases

Intuitively, one cannot construct arbitrarily many orthonormal bases when the maximal and minimal bases overlaps are specified. For example, it was known that there cannot be more than $d+1$ MUBs in \mathbb{C}^d (where $c_{\max}^{z,z'} = c_{\min}^{z,z'} = \frac{1}{d}$)⁴⁸. By making a connection to the Welch bounds³⁷, we can

upper bound the number of orthonormal bases using the function $\lambda(C)$ defined in Theorem 1 such that

$$m \leq \frac{d+1}{2} \left(1 + \sqrt{1 + \frac{8\lambda(C)(\lambda(C)-1)}{d^2-1}} \right) =: \bar{m}_d, \quad (13)$$

which is proven in Sec. S.IV of the Supplementary Information. For MUBs, we have $\lambda(C) = 1$, so eq. (13) becomes $m \leq d+1$, which agrees with the known upper bound⁴⁸. In general, the bound does not imply the existence of \bar{m}_d orthonormal bases. For instance, the existence of $d+1$ MUBs for non-prime-power dimensions d is still an open problem⁵¹. In Sec. S.I.1 of the Supplementary Information, we use this bound to show that eq. (5) is satisfied for our example.

Simple construction of three MUBs in any dimension

As a by-product of investigating the use of AMUBs for witnessing high-dimensional entanglement (see Sec. S.VI of the Supplementary Information), we discover a construction of three MUBs that has a simple analytic form and works for any dimension $d \in \mathbb{N}$. The nice feature about this is that it does not rely on (the tensor products of) the Wootters–Fields bases⁴⁸, which inevitably requires knowing the prime factorization of the dimension. Since factorizing a large integer is assumed to be hard (at least before any quantum device can properly implement Shor’s algorithm⁵² and the description of the Wootters–Fields bases can be non-trivial for large prime powers⁴⁸, constructing MUBs with the tensor products of the Wootters–Fields bases will require a certain amount of computational overhead, whereas our construction does not suffer from these problems despite having only three MUBs.

The explicit form of our three-MUBs construction is stated in the following lemma and its proof can be found in Sec. S.V of the Supplementary Information.

Lemma 2. For any $d \in \mathbb{N}$, the three orthonormal bases $\{|e_a^1\rangle = |a\rangle\}_{a=0}^{d-1}$, $\{|e_a^2\rangle\}_{a=0}^{d-1}$, and $\{|e_a^3\rangle\}_{a=0}^{d-1}$, with

$$|e_a^2\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} e^{i2\pi[\frac{aj}{d}+f(j)]} |j\rangle, \quad (14a)$$

$$|e_a^3\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} e^{i2\pi[\frac{(d-p')j^2}{2d}+\frac{aj}{d}+f(j)]} |j\rangle, \quad (14b)$$

where f is any real-valued function, $r \in \mathbb{N} \cup \{0\}$, and p is any odd prime such that $\gcd(d, p) = 1$ and $d > p'$, are mutually unbiased. The simplest example would be having $p' = 1$.

Since the function f (and to some degree, p') can be chosen freely, it can be optimized such that the relative phases in eqs. (14a) and (14b) are more easily realizable for different experimental setups. This flexibility is particularly useful in cases where the dimension of the Hilbert space in which the experiment operates can change over time (e.g., in scenarios where one has a dynamical encoding protocol that encodes information in different subspaces of the physical system at different times to protect against some time-dependent noise which affects various parts of the system in distinct ways) or the experiment has to measure different subsystems with distinct subspace dimensions at different times, as recalibration of the relative phases of our bases may require less drastic changes to the setup than using (the tensor product of) the Wootters–Fields bases. For the simplest example, if one needs to encode information or measure in 3 MUBs and the corresponding Hilbert space switches from dimension 7 to 6, then our simple construction only requires a slight change in the phases (especially with the free choices of $f(j)$ and p' for compensation), whereas using the Wootters–Fields bases will need to switch from the prime-dimension Wootters–Fields basis for $d = 7$ to the tensor products of the Wootters–Fields bases of dimensions 2 and 3, which introduce more drastic changes to the relative phases. For large d , the change to the relative phases can be even more drastic.

Discussion

Our results provide a fresh perspective on the longstanding problem of detecting entanglement using only a few, potentially restricted, measurement settings. Specifically, we introduced a family of Schmidt-number witnesses based on correlations in at least two coordinated local orthonormal bases that can be chosen arbitrarily. We established analytic upper bounds for the corresponding witness operators when evaluated on any bipartite state with a Schmidt number of at most k . The main advantage of our method is that the bounds depend solely on the absolute values of the overlaps between different measurement bases, but not on their relative phases, which are often inaccessible in experiments. These features of our witness simplify experimental requirements for certifying high-dimensional entanglement across many platforms. We demonstrated the effectiveness of our witness with two-qudit isotropic states and noisy purified thermal states. We also discussed the use of random measurement bases to witness Schmidt numbers. Finally, we compare our method with various existing approaches for certifying high-dimensional entanglement in Table 1.

As Corollary 1 suggests, one should aim at locally measuring in as many MUBs as possible to get the best performance of our witness. Sadly, the total number of MUBs is unknown for dimensions that are not prime powers⁵¹. In fact, given the prime factorization of the dimension $d = \prod_j p_j^{n_j}$ with $p_j^{n_j} < p_{j+1}^{n_{j+1}} \forall j$, (tensor products of) the Wootters–Fields construction only guarantees $p_1^{n_1} + 1$ MUBs to exist³⁸. Alternatively, if one can measure in bases that are nearly mutually unbiased, then one can construct $d+1$ AMUBs for any dimension d ⁴⁰. We constructed Schmidt-number witnesses based on the AMUBs proposed in ref. 40, but we did not observe any advantage of measuring in $4 \leq m \leq d+1$ AMUBs compared to measuring in three MUBs in the non-prime-powered dimensions $d = 6, 10, 14, 22$ (see Sec. S.VI of the Supplementary Information). The discovery of the simple three-MUBs construction in any dimension (Lemma 2) by modifying the AMUBs construction in ref. 40 suggests that there could be other constructions of AMUBs that are more suitable for witnessing Schmidt numbers and we leave finding such bases as an open problem. Furthermore, given the flexibility of our three-MUBs construction, it may even contribute to answering a longstanding mathematical problem: Are there more than three MUBs in even, non-prime-power dimensions such as $d = 6$?

Methods

Proof of Theorem 1

To prove Theorem 1, we start by stating the following propositions that we will need in the main proof.

Proposition 1. It holds that $A \otimes \mathbb{1}_d |\Phi_d^+\rangle = \mathbb{1}_d \otimes A^T |\Phi_d^+\rangle$ for all $A \in M(\mathbb{C}^d)$.

Proof. Let $A = \sum_{i,j=0}^{d-1} A_{ij} |i\rangle\langle j|$. Then,

$$\begin{aligned} A \otimes \mathbb{1}_d |\Phi_d^+\rangle &= \frac{1}{\sqrt{d}} \sum_{i,j,k=0}^{d-1} A_{ij} |i\rangle\langle j| \otimes |k\rangle\langle k| \\ &= \frac{1}{\sqrt{d}} \sum_{i,j=0}^{d-1} A_{ij} |i\rangle\langle j| \otimes \mathbb{1}_d, \end{aligned} \quad (15a)$$

$$\begin{aligned} \mathbb{1}_d \otimes A^T |\Phi_d^+\rangle &= \frac{1}{\sqrt{d}} \sum_{i,j,k=0}^{d-1} A_{ji} |k\rangle\langle i| \otimes |j\rangle\langle j| \\ &= \frac{1}{\sqrt{d}} \sum_{i,j=0}^{d-1} A_{ji} |j\rangle\langle i| \otimes \mathbb{1}_d, \end{aligned} \quad (15b)$$

so we indeed have $A \otimes \mathbb{1}_d |\Phi_d^+\rangle = \mathbb{1}_d \otimes A^T |\Phi_d^+\rangle$. \square

Proposition 2. Let $|\psi\rangle$ and $|\phi\rangle$ be normalized states. Then, the eigenvalues of $|\psi\rangle\langle\phi| + |\phi\rangle\langle\psi|$ are upper bounded by $|\langle\psi|\phi\rangle| + 1$ and lower bounded by $-(|\langle\psi|\phi\rangle| + 1)$.

Proof. Let $|\phi\rangle = a|\psi\rangle + b|\psi^\perp\rangle$ such that $|a|^2 + |b|^2 = 1$, $\langle\psi|\psi^\perp\rangle = 0$, and $\langle\psi|\psi\rangle = 1 = \langle\psi^\perp|\psi^\perp\rangle$. Then, $|\psi\rangle\langle\phi| + |\phi\rangle\langle\psi| = (a + a^*)|\psi\rangle\langle\psi| + b^*|\psi\rangle\langle\psi^\perp| + b|\psi^\perp\rangle\langle\psi|$, which has eigenvalues $\lambda_\pm = \text{Re}(a) \pm \sqrt{1 - \text{Im}(a)^2}$. Since $\text{Re}(a) \leq |a|$ and $\sqrt{1 - \text{Im}(a)^2} \leq 1$, we have $|\lambda_\pm| \leq |a| + 1 = |\langle\psi|\phi\rangle| + 1$. \square

We are now ready to state the formal proof of Theorem 1 which follows similar arguments for proving Result 1 in ref. 23 except here, the reference frame of party B relative to party A's is fixed by an arbitrary unitary and we cannot assume that $|\langle e_a^z | e_{a'}^{z'} \rangle|^2 = \frac{1}{d}$ for all $z \neq z'$.

Proof of Theorem 1. Let us define the witness operator

$$W = \sum_{z=1}^m \sum_{a=0}^{d-1} |e_a^z\rangle\langle e_a^z| \otimes |\tilde{e}_a^{z*}\rangle\langle \tilde{e}_a^{z*}| \quad (16)$$

so that $\text{Tr}(W\rho_{AB}) = S_d^{(m)}(\rho_{AB})$, where $|\tilde{e}_a^{z*}\rangle = U|e_a^{z*}\rangle$ and U is a fixed unitary that is the same for all a and z . Via the definition of $|\tilde{e}_a^{z*}\rangle$, we have $\sum_{a=0}^{d-1} (|e_a^z\rangle\langle e_a^z| \otimes |\tilde{e}_a^{z*}\rangle\langle \tilde{e}_a^{z*}|)(\mathbb{1}_d \otimes U)|\Phi_d^+\rangle = \sum_{a=0}^{d-1} (|e_a^z\rangle\langle e_a^z| \otimes U|e_a^{z*}\rangle\langle e_a^{z*}|)|\Phi_d^+\rangle = \sum_{a=0}^{d-1} |e_a^z\rangle\langle e_a^z| \otimes |\tilde{e}_a^{z*}\rangle\langle \tilde{e}_a^{z*}|(\mathbb{1}_d \otimes U)|\Phi_d^+\rangle = (\mathbb{1}_d \otimes U)|\Phi_d^+\rangle =: |\tilde{\Phi}_d^+\rangle$, where we have used Proposition 1 in the second step. Hence, we have $W|\tilde{\Phi}_d^+\rangle = m|\tilde{\Phi}_d^+\rangle$. Since W is positive semi-definite, it has a spectral decomposition: $W = m|\tilde{\Phi}_d^+\rangle\langle \tilde{\Phi}_d^+| + \sum_{i=2}^{d^2} \lambda_i |\lambda_i\rangle\langle \lambda_i|$ where all normalized eigenvectors $|\lambda_i\rangle$ are orthogonal to $|\tilde{\Phi}_d^+\rangle$.

Next, we will derive an upper bound for all the eigenvalues λ_i with $i = 2, \dots, d^2$. To do this, we consider the operator

$$\begin{aligned} W^2 &= W + \sum_{z \neq z'} \sum_{a, a'} |\langle e_a^z | e_{a'}^{z'} \rangle|^2 |e_a^z \tilde{e}_{a'}^{z*}\rangle\langle e_{a'}^{z'} \tilde{e}_a^{z*}| \\ &= W + \sum_{z \neq z'} c_{\min}^{z, z'} \mathbb{1}_1 + T_2, \end{aligned} \quad (17)$$

with $T_1^{z, z'} = \sum_{a, a'} |e_a^z \tilde{e}_{a'}^{z*}\rangle\langle e_{a'}^{z'} \tilde{e}_a^{z*}| = d|\tilde{\Phi}_d^+\rangle\langle \tilde{\Phi}_d^+|$ since $V \otimes V^*$ with $V = \sum_{j=0}^{d-1} |e_j^z\rangle\langle j|$ is a symmetry of $|\Phi_d^+\rangle$ by Proposition 1, and

$$\begin{aligned} T_2 &= \sum_{z \neq z'} \sum_{a, a'} (|\langle e_a^z | e_{a'}^{z'} \rangle|^2 - c_{\min}^{z, z'}) |e_a^z \tilde{e}_{a'}^{z*}\rangle\langle e_{a'}^{z'} \tilde{e}_a^{z*}| \\ &= \sum_{z \neq z'} \sum_{a, a'} (|\langle e_a^z | e_{a'}^{z'} \rangle|^2 - c_{\min}^{z, z'}) \frac{1}{2} (|e_a^z \tilde{e}_{a'}^{z*}\rangle\langle e_{a'}^{z'} \tilde{e}_a^{z*}| + \text{H.c.}), \end{aligned} \quad (18)$$

where we use the fact that $|\langle e_a^z | e_{a'}^{z'} \rangle| = |\langle e_{a'}^{z'} | e_a^z \rangle| \forall a, a', z, z'$ and “H.c.” stands for the Hermitian conjugate of the previous term. Then, we use (i) $|\langle e_a^z | e_{a'}^{z'} \rangle|^2 - c_{\min}^{z, z'} \geq 0$, (ii) $|e_a^z \tilde{e}_{a'}^{z*}\rangle\langle e_{a'}^{z'} \tilde{e}_a^{z*}| + \text{H.c.} \leq \lambda_{\max}(|e_a^z \tilde{e}_{a'}^{z*}\rangle\langle e_{a'}^{z'} \tilde{e}_a^{z*}| + \text{H.c.}) \mathbb{1}_{d^2}$, where $\lambda_{\max}(A)$ denotes the largest eigenvalue of A , (iii) $\lambda_{\max}(\sum_i A_i) \leq \sum_i \lambda_{\max}(A_i)$ for all $A_i \in \text{Herm}(\mathbb{C}^d)^{53}$, and (iv) Proposition 2 to obtain

$$\begin{aligned} T_2 &\leq \frac{1}{2} \sum_{z \neq z'} \sum_{a, a'} (|\langle e_a^z | e_{a'}^{z'} \rangle|^2 - c_{\min}^{z, z'}) \lambda_{\max}(|e_a^z \tilde{e}_{a'}^{z*}\rangle\langle e_{a'}^{z'} \tilde{e}_a^{z*}| + \text{H.c.}) \mathbb{1}_{d^2} \\ &\leq \frac{1}{2} \sum_{z \neq z'} \sum_{a, a'} (|\langle e_a^z | e_{a'}^{z'} \rangle|^2 - c_{\min}^{z, z'}) (|\langle e_a^z | e_{a'}^{z'} \rangle|^2 + 1) \mathbb{1}_{d^2}. \end{aligned} \quad (19)$$

Finally, we use the equality $\sum_{a'=0}^{d-1} |\langle e_a^z | e_{a'}^{z'} \rangle|^2 = 1$ to get

$$\begin{aligned} T_2 &\leq \frac{1}{2} \sum_{z \neq z'} \left[\sum_a (1 - c_{\min}^{z, z'} - c_{\min}^{z, z'} d) + \sum_{a, a'} |\langle e_a^z | e_{a'}^{z'} \rangle|^4 \right] \mathbb{1}_{d^2} \\ &= \frac{d}{2} \sum_{z \neq z'} \left[1 - (d+1)c_{\min}^{z, z'} + \frac{1}{d} \sum_{a, a'} |\langle e_a^z | e_{a'}^{z'} \rangle|^4 \right] \mathbb{1}_{d^2} \\ &=: \frac{d}{2} \sum_{z \neq z'} G^{z, z'} \mathbb{1}_{d^2}. \end{aligned} \quad (20)$$

After combining eqs. (17) and (20), we obtain

$$W^2 \leq W + d \sum_{z \neq z'} \left(c_{\min}^{z, z'} |\tilde{\Phi}_d^+\rangle\langle \tilde{\Phi}_d^+| + \frac{1}{2} G^{z, z'} \mathbb{1}_{d^2} \right). \quad (21)$$

Since $W^2 = m^2 |\tilde{\Phi}_d^+\rangle\langle \tilde{\Phi}_d^+| + \sum_{i=2}^{d^2} \lambda_i^2 |\lambda_i\rangle\langle \lambda_i|$ and due to eq. (21), we have that $\lambda_i^2 \leq \lambda_i + \frac{d}{2} \sum_{z \neq z'} G^{z, z'}$ for $i = 2, \dots, d^2$, which implies that $\lambda_i \leq \frac{1}{2} \left(1 + \sqrt{1 + 2d \sum_{z \neq z'} G^{z, z'}} \right) =: \lambda(C)$. Since $G^{z, z'} \geq 0 \forall z \neq z'$ [see eq. (19)], $\lambda(C) \geq 1$. On the other hand, we know that $\lambda_{\max}(W) = \lambda_{\max}(\sum_{z=1}^m \sum_{a=0}^{d-1} |e_a^z\rangle\langle e_a^z| \otimes |\tilde{e}_a^{z*}\rangle\langle \tilde{e}_a^{z*}|) \leq \sum_z \lambda_{\max}(\sum_a |e_a^z\rangle\langle e_a^z| \otimes |\tilde{e}_a^{z*}\rangle\langle \tilde{e}_a^{z*}|) = m$, so $\lambda_i \leq T(C) := \min\{\lambda(C), m\}$. Therefore, with $W|\tilde{\Phi}_d^+\rangle = m|\tilde{\Phi}_d^+\rangle$, we have that

$$W \leq (m - T(C)) |\tilde{\Phi}_d^+\rangle\langle \tilde{\Phi}_d^+| + T(C) \mathbb{1}_{d^2}. \quad (22)$$

Finally, we arrive at our bound in eq. (4) in Theorem 1:

$$\begin{aligned} S_d^{(m)}(\rho_{AB}) &= \text{Tr}(W\rho_{AB}) \leq (m - T(C)) \mathcal{F}(\rho_{AB}) + T(C) \\ &\leq \frac{k(m - T(C))}{d} + T(C), \end{aligned} \quad (23)$$

where we have used the fact that $\langle \tilde{\Phi}_d^+ | \rho_{AB} | \tilde{\Phi}_d^+ \rangle \leq \mathcal{F}(\rho_{AB}) \leq \frac{k}{d}$ for all bipartite state ρ_{AB} of equal local dimension d and Schmidt number at most k^{24} . The fidelity lower bound in eq. (5) can also be obtained by rearranging the first line of eq. (23) and is non-trivial only if $T(C) < S_d^{(m)}(\rho_{AB})$. Otherwise, we set $\mathcal{F}_m = 0$ as $\mathcal{F}(\rho_{AB}) \geq 0$ always holds. \square

Proof of Lemma 1

To prove Lemma 1, we need the following proposition which is proven in “Proof of Proposition 3”.

Proposition 3. The optimal solution to the optimization problem: $\max \sum_{i=1}^{d^2} x_i^4$ subject to $\sum_{i=jd+1}^{jd+d} x_i^2 = 1$ for $j = 0, \dots, d-1$, and $0 \leq \sqrt{c_{\min}} \leq x_i \leq \sqrt{c_{\max}} \leq 1 \forall i$ is $d[Lc_{\max}^2 + (d-L-1)c_{\min}^2 + [1 - Lc_{\max} - (d-L-1)c_{\min}]^2]$, where

$$L = \begin{cases} \left\lfloor \frac{1 - c_{\min} d}{c_{\max} - c_{\min}} \right\rfloor & \text{if } c_{\max} > c_{\min}, \\ d & \text{if } c_{\max} = c_{\min}. \end{cases} \quad (24)$$

Proof of Lemma 1. We will prove that $\overline{T}(\overline{C}) \geq T(C)$ for all bases overlaps C so that

$$\begin{aligned} S_d^{(m)}(\rho_{AB}) &\leq \mathcal{B}_k = (1 - \frac{k}{d})T(C) + \frac{km}{d} \\ &\leq (1 - \frac{k}{d})\overline{T}(\overline{C}) + \frac{km}{d} \end{aligned} \quad (25)$$

for all $k \leq d$ as in eq. (6). This boils down to showing that $\sum_{a, a'} |\langle e_a^z | e_{a'}^{z'} \rangle|^4 \leq \Omega^{z, z'} d$ which implies $G^{z, z'} \leq \overline{G}^{z, z'} \forall z, z'$.

For every pair of distinct bases z, z' , we want to maximize $\sum_{a, a'} |\langle e_a^z | e_{a'}^{z'} \rangle|^4$ given that $\sum_{a'} |\langle e_a^z | e_{a'}^{z'} \rangle|^2 = 1 \forall a$ and $0 \leq \sqrt{c_{\min}} \leq |\langle e_a^z | e_{a'}^{z'} \rangle| \leq \sqrt{c_{\max}} \leq 1 \forall a, a'$. By setting $x_i = |\langle e_a^z | e_{a'}^{z'} \rangle|$ and $i = da + a' + 1$, we can apply Proposition 3 to obtain the maximum value, $\Omega^{z, z'} d$. Hence, $\overline{T}(\overline{C}) \geq T(C)$ and eq. (6) holds. Finally, the fidelity lower bound in eq. (8) can be obtained in a similar fashion as in the proof of Theorem 1. The bound is non-trivial only if $\overline{T}(\overline{C}) < S_d^{(m)}(\rho_{AB})$. Otherwise, we set $\overline{\mathcal{F}}_m = 0$ since $\mathcal{F}(\rho_{AB}) \geq 0$ always holds. \square

Proof of Proposition 3. A general constrained optimization problem can be written in the following form⁵⁴.

Problem 1. Let $\vec{x} \in \mathbb{R}^d$. A constrained optimization problem can be written as

$$\begin{aligned} & \text{minimize} && f(\vec{x}) \\ & \text{subject to} && h_1(\vec{x}) = 0, \dots, h_m(\vec{x}) = 0, \\ & && g_1(\vec{x}) \leq 0, \dots, g_r(\vec{x}) \leq 0, \end{aligned} \quad (26)$$

where f, h_i, g_j are functions mapping from \mathbb{R}^d to \mathbb{R} . The feasible set $X \subset \mathbb{R}^d$ is composed of all the $\vec{x} \in \mathbb{R}^d$ that satisfy all the equality and inequality constraints. The associated Lagrangian of the problem is given by

$$L(\vec{x}, \vec{\lambda}, \vec{\mu}) = f(\vec{x}) + \sum_{i=1}^m \lambda_i h_i(\vec{x}) + \sum_{j=1}^r \mu_j g_j(\vec{x}), \quad (27)$$

where $\lambda_i, \mu_j \in \mathbb{R}$ are Lagrange multipliers.

It is useful to give the following definitions which we quote directly from ref. 54 before stating Lemma 3.

Definition 1. (Local minimum). A vector $\vec{x}^* \in X$ is a local minimum of the objective function f over the feasible set X if there exists an $\epsilon > 0$ such that $f(\vec{x}^*) \leq f(\vec{x})$ for all $\vec{x} \in X$ where $\|\vec{x} - \vec{x}^*\| < \epsilon$.

Definition 2. (Active constraints). The set of active inequality constraints $A(\vec{x})$ at a point $\vec{x} \in X$ is the set of indices of the inequality constraints that are satisfied as equalities at \vec{x} , i.e., $A(\vec{x}) = \{j | g_j(\vec{x}) = 0\}$.

Definition 3. (Regularity). A feasible vector \vec{x} is regular if the gradients of all the equality constraints $\nabla h_i(\vec{x}), i = 1, \dots, m$, and the gradients of all the active inequality constraints $\nabla g_j(\vec{x}), j \in A(\vec{x})$, are linearly independent.

Lemma 3. (Proposition 3.3.1 in ref. 54). Let \vec{x}^* be a local minimum of Problem 1 where f, h_i, g_j are continuously differentiable functions from \mathbb{R}^d to \mathbb{R} , and assume that \vec{x}^* is regular. Then, there exist unique Lagrange multiplier vectors $\vec{\lambda}^* = (\lambda_1^*, \dots, \lambda_m^*)^T \in \mathbb{R}^m$ and $\vec{\mu}^* = (\mu_1^*, \dots, \mu_r^*)^T \in \mathbb{R}^r$, such that

$$\begin{cases} \nabla_x L(\vec{x}^*, \vec{\lambda}^*, \vec{\mu}^*) = \vec{0} \\ \mu_j^* \geq 0, & j = 1, \dots, r, \\ \mu_j^* = 0, & \forall j \notin A(\vec{x}^*), \end{cases} \quad (28)$$

where $A(\vec{x}^*)$ is the set of active constraints at \vec{x}^* .

Proof of Proposition 3. We will first translate our optimization problem into the form in Problem 1, where we have $f(\vec{x}) = -\sum_{i=1}^d x_i^4$, $h_{j+1}(\vec{x}) = \sum_{i=jd+1}^{jd+d} x_i^2 - 1$, $g_{2jd+k+1}(\vec{x}) = x_{jd+k+1} - \sqrt{c_{\max}}$, and $g_{(2j+1)d+k+1}(\vec{x}) = \sqrt{c_{\min}} - x_{jd+k+1}$ for $j, k = 0, \dots, d-1$, where $0 \leq c_{\min} \leq c_{\max} \leq 1$. This is in fact a sum of d independent optimization problems of identical form, which simplifies our whole optimization problem to:

$$\begin{aligned} & \text{minimize} && f(\vec{x}) = -d \sum_{i=1}^d x_i^4 \\ & \text{subject to} && h(\vec{x}) = \sum_{i=1}^d x_i^2 - 1 = 0, \\ & && g_k(\vec{x}) = x_k - \sqrt{c_{\max}} \leq 0, \\ & && g_{d+k}(\vec{x}) = \sqrt{c_{\min}} - x_k \leq 0, \quad k = 1, \dots, d, \end{aligned} \quad (29)$$

where we redefine the objective function $f(\vec{x})$. The associated Lagrangian is given by

$$\begin{aligned} L(\vec{x}, \lambda, \vec{\mu}) = & \sum_{i=1}^d [-dx_i^4 + \lambda x_i^2 + (\mu_i - \mu_{i+d})x_i] \\ & - \lambda - \sum_{i=1}^d (\sqrt{c_{\max}}\mu_i - \sqrt{c_{\min}}\mu_{i+d}), \end{aligned} \quad (30)$$

where $\lambda, \mu_j \in \mathbb{R}$. Let us determine which \vec{x} is regular by evaluating the following gradients:

$$\nabla h(\vec{x}) = \sum_i 2x_i|i\rangle, \quad \nabla g_i(\vec{x}) = |i\rangle, \quad \nabla g_{i+d}(\vec{x}) = -|i\rangle. \quad (31)$$

If $g_i(\vec{x}) \leq 0$ is active (i.e., $x_i = \sqrt{c_{\max}}$), then $g_{i+d}(\vec{x}) \leq 0$ for the same i must be inactive unless $c_{\min} = c_{\max}$, and vice versa. Note that the only feasible solution of the case when $c_{\min} = c_{\max}$ are non-regular since both $g_i(\vec{x}) \leq 0$ and $g_{i+d}(\vec{x}) \leq 0$ are active for all i , so $\nabla h(\vec{x}), \nabla g_i(\vec{x})$, and $\nabla g_{i+d}(\vec{x})$ for $i = 1, \dots, d$ are linearly dependent. Also, if $\sqrt{c_{\min}} < x_i < \sqrt{c_{\max}}$, then both $g_i(\vec{x}) \leq 0$ and $g_{i+d}(\vec{x}) \leq 0$ are inactive. Hence, for \vec{x}^* to be regular, the following must hold:

- At least one component x_i^* must satisfy $\sqrt{c_{\min}} < x_i^* < \sqrt{c_{\max}}$ so that both $g_i(\vec{x}^*) \leq 0$ and $g_{i+d}(\vec{x}^*) \leq 0$ are inactive.
- In case $c_{\min} = 0$, if at least one component $x_i^* = \sqrt{c_{\min}} = 0$ so that the i -th component of $\nabla h(\vec{x}^*)$ is 0 while $\nabla g_{i+d}(\vec{x}^*) = -|i\rangle$, then condition (i) is not necessary. If $x_i^* > 0 \forall i$, condition (i) must hold.

Since the functions f, h, g_i, g_{i+d} for all $i = 1, \dots, d$ are continuously differentiable, all regular local minima of Problem (29) must satisfy Lemma 3. Let us evaluate

$$\nabla_x L = \sum_{i=1}^d (-4dx_i^3 + 2\lambda x_i + \mu_i - \mu_{i+d})|i\rangle, \quad (32)$$

and consider the case where the i -th component of a regular local minimum \vec{x}^* satisfies $\sqrt{c_{\min}} < x_i^* < \sqrt{c_{\max}}$. By Lemma 3, $\mu_i^* = \mu_{i+d}^* = 0$, implying that $-4d(x_i^*)^3 + 2\lambda^* x_i^* = 0$. Hence,

$$\lambda^* = 2d(x_i^*)^2. \quad (33)$$

Since λ^* is a parameter independent of the index i , we can constrain all components of \vec{x}^* that lie within the interval, $(\sqrt{c_{\min}}, \sqrt{c_{\max}})$, with this common parameter. According to eq. (33), $x_i^* = x_j^* = \sqrt{\lambda^*/(2d)}$ for all i, j such that $\sqrt{c_{\min}} < x_i^*, x_j^* < \sqrt{c_{\max}}$. Hence, for any regular local minimum \vec{x}^* of the optimization problem (29), each component x_i^* can only take one of the three possible values: $\sqrt{c_{\min}}, \sqrt{\chi}, \sqrt{c_{\max}}$, where $\chi \in (c_{\min}, c_{\max})$.

Therefore, we can translate our optimization problem of (29) into a much simplified form:

$$\begin{aligned} & \text{maximize} && d[Lc_{\max}^2 + \bar{L}\chi^2 + (d-L-\bar{L})c_{\min}^2] \\ & \text{subject to} && Lc_{\max} + \bar{L}\chi + (d-L-\bar{L})c_{\min} = 1, \\ & && 0 \leq L + \bar{L} \leq d, \quad L, \bar{L} \in \mathbb{N}, \\ & && 0 \leq c_{\min} < \chi < c_{\max} \leq 1, \end{aligned} \quad (34)$$

where we converted our problem back to a maximization problem. Clearly, the optimal solution can be obtained by maximizing L while satisfying all constraints, including eq. (34) which can be rearranged into:

$$L = \frac{1 - c_{\min}d}{c_{\max} - c_{\min}} - \bar{L} \frac{\chi - c_{\min}}{c_{\max} - c_{\min}}. \quad (35)$$

Since the last fraction lies within the interval $(0, 1)$, the maximum value allowed for L is $\lfloor \frac{1-c_{\min}d}{c_{\max}-c_{\min}} \rfloor$, leaving either $\bar{L} = 0$ if $\frac{1-c_{\min}d}{c_{\max}-c_{\min}} \in \mathbb{N}$, or $\bar{L} = 1$ with $\chi = 1 - Lc_{\max} - (d - L - 1)c_{\min}$ otherwise.

Next, we consider the remaining cases: (1) regular local minima \vec{x}^* with no components satisfying $\sqrt{c_{\min}} < x_i^* < \sqrt{c_{\max}}$ when $c_{\min} = 0$, and (2) non-regular points \vec{x} with each component $x_i \in \{\sqrt{c_{\min}} > 0, \sqrt{c_{\max}}\}$ [see conditions (i) and (ii)]. Note that the case where $c_{\min} = c_{\max}$ is included here. Similar to the previous regular cases, we can simplify our optimization problem to:

$$\begin{aligned} & \text{maximize } d[Lc_{\max}^2 + (d - L)c_{\min}^2] \\ & \text{subject to } Lc_{\max} + (d - L)c_{\min} = 1, \\ & 0 \leq L \leq d, L \in \mathbb{N}, 0 \leq c_{\min} \leq c_{\max} \leq 1. \end{aligned} \quad (36)$$

If $c_{\min} < c_{\max}$, the problem has a feasible optimum only if $L = \frac{1-c_{\min}d}{c_{\max}-c_{\min}} \in \mathbb{N}$. If $c_{\min} = c_{\max}$, the problem has a feasible solution only if $c_{\min} = c_{\max} = \frac{1}{d}$.

Finally, since the global optimum to our initial Problem (29) is the minimum over the set composed of all feasible points fulfilling Lemma 3 (a set containing all regular local minima) together with all irregular feasible solutions, we can conclude that the global optimum \vec{x}^* satisfies: $x_i^* = \sqrt{c_{\max}}$ for $i = 1, \dots, L$, $x_j^* = \sqrt{c_{\min}}$ for $j = L + 1, \dots, d - 1$, and $x_d^* = \sqrt{1 - Lc_{\max} - (d - L - 1)c_{\min}}$, where

$$L = \begin{cases} \left\lfloor \frac{1-c_{\min}d}{c_{\max}-c_{\min}} \right\rfloor & \text{if } c_{\max} > c_{\min}, \\ d & \text{if } c_{\max} = c_{\min}. \end{cases} \quad (37)$$

□

Data availability

Data sharing is not applicable to this article as no datasets were generated or analysed during the current study.

Received: 30 July 2024; Accepted: 10 February 2025;

Published online: 19 March 2025

References

- Bennett, C. H. & Wiesner, S. J. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. *Phys. Rev. Lett.* **69**, 2881–2884 (1992).
- Bennett, C. H. et al. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.* **70**, 1895–1899 (1993).
- Buhrman, H., Cleve, R., Massar, S. & de Wolf, R. Nonlocality and communication complexity. *Rev. Mod. Phys.* **82**, 665–698 (2010).
- Scarani, V. et al. The security of practical quantum key distribution. *Rev. Mod. Phys.* **81**, 1301–1350 (2009).
- Xu, F., Ma, X., Zhang, Q., Lo, H.-K. & Pan, J.-W. Secure quantum key distribution with realistic devices. *Rev. Mod. Phys.* **92**, 025002 (2020).
- Degen, C. L., Reinhard, F. & Cappellaro, P. Quantum sensing. *Rev. Mod. Phys.* **89**, 035002 (2017).
- Giovannetti, V., Lloyd, S. & Maccone, L. Advances in quantum metrology. *Nat. Photonics* **5**, 222 (2011).
- Jozsa, R. & Linden, N. On the role of entanglement in quantum-computational speed-up. *Proc. Roy. Soc. A Math. Phys.* **459**, 2011–2032 (2003).
- Friis, N., Vitagliano, G., Malik, M. & Huber, M. Entanglement certification from theory to experiment. *Nat. Rev. Phys.* **1**, 72–87 (2019).
- Bavaresco, J. et al. Measurements in two bases are sufficient for certifying high-dimensional entanglement. *Nat. Phys.* **14**, 1032–1037 (2018).
- Hrmo, P. et al. Native qudit entanglement in a trapped ion quantum processor. *Nat. Commun.* **14**, 2242 (2023).
- Doda, M. et al. Quantum key distribution overcoming extreme noise: simultaneous subspace coding using high-dimensional entanglement. *Phys. Rev. Appl.* **15**, 034003 (2021).
- Ndagano, B. et al. Imaging and certifying high-dimensional entanglement with a single-photon avalanche diode camera. *npj Quant. Inf.* **6**, 94 (2020).
- Defienne, H., Ndagano, B., Lyons, A. & Faccio, D. Polarization entanglement-enabled quantum holography. *Nat. Phys.* **17**, 591–597 (2021).
- Cameron, P. et al. Adaptive optical imaging with entangled photons. *Science* **383**, 1142–1148 (2024).
- Lanyon, B. P. et al. Simplifying quantum logic using higher-dimensional Hilbert spaces. *Nat. Phys.* **5**, 134–140 (2009).
- Amico, L., Fazio, R., Osterloh, A. & Vedral, V. Entanglement in many-body systems. *Rev. Mod. Phys.* **80**, 517–576 (2008).
- 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**, 143–224 (2008).
- Eisert, J., Cramer, M. & Plenio, M. B. Colloquium: Area laws for the entanglement entropy. *Rev. Mod. Phys.* **82**, 277–306 (2010).
- Spengler, C., Huber, M., Brierley, S., Adaktylos, T. & Hiesmayr, B. C. Entanglement detection via mutually unbiased bases. *Phys. Rev. A* **86**, 022311 (2012).
- Erker, P., Krenn, M. & Huber, M. Quantifying high dimensional entanglement with two mutually unbiased bases. *Quantum* **1**, 22 (2017).
- Herrera Valencia, N. et al. High-dimensional pixel entanglement: efficient generation and certification. *Quantum* **4**, 376 (2020).
- Morelli, S., Huber, M. & Tavakoli, A. Resource-efficient high-dimensional entanglement detection via symmetric projections. *Phys. Rev. Lett.* **131**, 170201 (2023).
- Terhal, B. M. & Horodecki, P. Schmidt number for density matrices. *Phys. Rev. A* **61**, 040301(R) (2000).
- Berta, M., Christandl, M., Colbeck, R., Renes, J. M. & Renner, R. The uncertainty principle in the presence of quantum memory. *Nat. Phys.* **6**, 659–662 (2010).
- Coles, P. J., Berta, M., Tomamichel, M. & Wehner, S. Entropic uncertainty relations and their applications. *Rev. Mod. Phys.* **89**, 015002 (2017).
- Devetak, I. & Winter, A. Distillation of secret key and entanglement from quantum states. *Proc. R. Soc. Lond. A* **461**, 207–235 (2005).
- Bennett, C. H., Di Vincenzo, D. P., Smolin, J. A. & Wootters, W. K. Mixed-state entanglement and quantum error correction. *Phys. Rev. A* **54**, 3824 (1996).
- Horodecki, M., Horodecki, P. & Horodecki, R. General teleportation channel, singlet fraction and quasidistillation. *Phys. Rev. A* **60**, 1888 (1999).
- Ivonović, I. D. Geometrical description of quantal state determination. *J. Phys. A Math. Gen.* **14**, 3241 (1981).
- Chang, K.-C. et al. Experimental high-dimensional entanglement certification and quantum steering with time-energy measurements. *Quant. Phys.* <https://doi.org/10.48550/arXiv.2310.20694> (2024).
- Euler, N. & Gärtner, M. Detecting high-dimensional entanglement in cold-atom quantum simulators. *PRX Quantum* **4**, 040338 (2023).
- Blumenson, L. E. A Derivation of n-dimensional spherical coordinates. *Am. Math. Mon.* **67**, 63–66 (1960).
- Milman, V. D. & Schechtman, G. *Asymptotic Theory of Finite Dimensional Normed Spaces* 1st edn, Vol. 160 (Springer, Berlin, Heidelberg, 1986).
- Ledoux, M. *The Concentration of Measure Phenomenon, Mathematical Surveys and Monographs*, Vol. 192 (American Mathematical Society, 2001).
- Hayden, P., Leung, D. W. & Winter, A. Aspects of generic entanglement. *Commun. Math. Phys.* **265**, 95–117 (2006).
- Welch, L. R. Lower bounds on the maximum cross correlation of signals (Corresp.). *IEEE Trans. Inf. Theory* **20**, 397–399 (1974).

38. Prat Colomer, M., Mortimer, L., Frérot, I., Farkas, M. & Acín, A. Three numerical approaches to find mutually unbiased bases using bell inequalities. *Quantum* **6**, 778 (2022).
39. Dirichlet, J. P. G. L. Sur la convergence des séries trigonométriques qui servent à représenter une fonction arbitraire entre des limites données. *J. für die Reine Und Angewandte Mathematik* **4**, 157–169 (1829).
40. Shparlinski, I. E. & Winterhof, A. Constructions of approximately mutually unbiased bases. In *LATIN 2006: Theoretical Informatics* (eds. Correa, J.R., Hevia, A., and Kiwi, M) 793–799 (Springer, Berlin, Heidelberg, 2006).
41. Cochrane, T. & Peral, J. C. An asymptotic formula for a trigonometric sum of Vinogradov. *J. Number Theory* **91**, 1–19 (2001).
42. Bertrand, J. Mémoire sur le nombre de valeurs que peut prendre une fonction quand on y permute les lettres qu'elle renferme. *J. de l'École Royale Polytech.* **18**, 123–140 (1845).
43. Chebyshev, P. Mémoire sur les nombres premiers. *J. de Mathématiques Pures et appliquées* **1**, 366–390 (1852).
44. Sloane, N. J. A. & The OEIS Foundation Inc. *The Online Encyclopedia of Integer Sequences*. <http://oeis.org/> (2025).
45. Gross, D. Hudson's theorem for finite-dimensional quantum systems. *J. Math. Phys.* **47**, 122107 (2006).
46. Kueng, R. & Gross, D. Qubit stabilizer states are complex projective 3-designs. *Quant. Phys.* <https://doi.org/10.48550/arXiv.1510.02767> (2015).
47. Berndt, B. C., Evans, R. J. & Williams, K. S. *Gauss and Jacobi Sums, Wiley-Interscience and Canadian Mathematics Series of Monographs and Texts* 1st edn, Vol. 600 (Wiley, New York, 1998).
48. Wootters, W. K. & Fields, B. D. Optimal state-determination by mutually unbiased measurements. *Ann. Phys.* **191**, 363–381 (1989).
49. Rungta, P. & Caves, C. M. Concurrence-based entanglement measures for isotropic states. *Phys. Rev. A* **67**, 012307 (2003).
50. Lee, S., Chi, D. P., Oh, S. D. & Kim, J. Convex-roof extended negativity as an entanglement measure for bipartite quantum systems. *Phys. Rev. A* **68**, 062304 (2003).
51. Durt, T., Englert, B.-G., Bengtsson, I. & Życzkowski, K. On mutually unbiased bases. *Int. J. Quant. Inf.* **08**, 535–640 (2010).
52. Shor, P. W. Algorithms for quantum computation: discrete logarithms and factoring. In *Proc. 35th Annual Symposium on Foundations of Computer Science* 124–134 (IEEE, 1994).
53. Bhatia, R. *Matrix Analysis* 1st edn, Vol. 349 (Springer, Berlin, 1996).
54. Bertsekas, D. P. *Nonlinear Programming* 2nd ed (Athena Scientific, Massachusetts, 1999).
55. Morelli, S., Yamasaki, H., Huber, M. & Tavakoli, A. Entanglement detection with imprecise measurements. *Phys. Rev. Lett.* **128**, 250501 (2022).
56. Bertlmann, R. A. & Friis, N. *Modern Quantum Theory—From Quantum Mechanics to Entanglement and Quantum Information*, Vol. 1040 (Oxford University Press, Oxford, U.K, 2023).
57. Collins, D., Gisin, N., Linden, N., Massar, S. & Popescu, S. Bell inequalities for arbitrarily high-dimensional systems. *Phys. Rev. Lett.* **88**, 040404 (2002).
58. Dada, A. C., Leach, J., Buller, G. S., Padgett, M. J. & Andersson, E. Experimental high-dimensional two-photon entanglement and violations of generalized bell inequalities. *Nat. Phys.* **7**, 677–680 (2011).
59. Braunstein, S. L., Mann, A. & Revzen, M. Maximal violation of bell inequalities for mixed states. *Phys. Rev. Lett.* **68**, 3259 (1992).
60. Acín, A., Durt, T., Gisin, N. & Latorre, J. I. Quantum nonlocality in two three-level systems. *Phys. Rev. A* **65**, 052325 (2002).
61. Wyderka, N. & Ketterer, A. Probing the geometry of correlation matrices with randomized measurements. *PRX Quant.* **4**, 020325 (2023).
62. Nakata, Y. et al. Quantum circuits for exact unitary t -designs and applications to higher-order randomized benchmarking. *PRX Quant.* **2**, 030339 (2021).
63. Harrow, A. W. & Mehraban, S. Approximate unitary t -designs by short random quantum circuits using nearest-neighbor and long-range gates. *Commun. Math. Phys.* **401**, 1531–1626 (2023).

Acknowledgements

We thank Dimpi Thakuria, Paul Erker, and Alexandra Bergmayr for insightful discussions about practical challenges in experimental entanglement certification. We also thank Matej Pivoluska for the helpful discussion regarding Lemma 1 in ref. 22 (Proposition S.1 in the Supplementary Information). In addition, we thank Christopher J. Turner for pointing out that the phase freedom in our original 3-MUBs construction can be further generalized (Lemma 2) and Richard Kueng for making us aware of the connection between our 3-MUBs construction and properties of stabilizer states in refs. 45,46. This research was funded in whole or in part by the Austrian Science Fund (FWF) [10.55776/P36478]. For open access purposes, the author has applied a CC BY public copyright license to any author accepted manuscript version arising from this submission. We further acknowledge support from the Austrian Federal Ministry of Education, Science and Research via the Austrian Research Promotion Agency (FFG) through the flagship project FO999897481 (HPQC), the project FO999914030 (MUSIQ), and the project FO999921407 (HDcode) funded by the European Union—NextGenerationEU, from the European Research Council (Consolidator grant ‘Cocoquest’ 101043705), and the Horizon-Europe research and innovation programme under grant agreement No 101070168 (HyperSpace).

Author contributions

N.K.H.L. discovered and produced all the results in this work. N.F. provided the ideas that led to the consideration of the examples with purified thermal states mixed with white noise, the analytic comparison of our witnesses with the ones of ref. 10, and random measurement bases. M.H. provided the idea that led to the study of applicability of AMUBs. All authors discussed the results and contributed to the writing of the final manuscript.

Competing interests

The authors declare no competing interests.

Additional information

Supplementary information The online version contains supplementary material available at <https://doi.org/10.1038/s41534-025-00990-6>.

Correspondence and requests for materials should be addressed to Nicky Kai Hong Li.

Reprints and permissions information is available at <http://www.nature.com/reprints>

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

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 licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence 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 licence, visit <http://creativecommons.org/licenses/by/4.0/>.

© The Author(s) 2025