OPEN

(Check for updates

Zero uncertainty states in the presence of quantum memory

Huangjun Zhu^{1,2,3,4}⊠

ARTICLE

The uncertainty principle imposes a fundamental limit on predicting the measurement outcomes of incompatible observables even if complete classical information of the system state is known. The situation is different if one can build a quantum memory entangled with the system. Zero uncertainty states (in contrast with minimum uncertainty states) are peculiar quantum states that can eliminate uncertainties of incompatible von Neumann observables once assisted by suitable measurements on the memory. Here we determine all zero uncertainty states of any given set of nondegenerate observables and determine the minimum entanglement required. It turns out all zero uncertainty states are maximally entangled in a generic case, and vice versa, even if these observables are only weakly incompatible. Our work establishes a simple and precise connection between zero uncertainty and maximum entanglement, which is of interest to foundational studies and practical applications, including quantum certification and verification.

npj Quantum Information (2021)7:47; https://doi.org/10.1038/s41534-021-00384-4

INTRODUCTION

The uncertainty principle represents a key distinction between quantum mechanics and classical mechanics and is still a focus of current research¹⁻⁴. It imposes a fundamental limit on our ability to predict the measurement outcomes of incompatible observables, such as position and momentum^{5,6}. However, uncertainty relations have to be modified in the presence of a quantum memory because entanglement between the memory and system can reduce the uncertainty⁷⁻¹². Besides foundational significance, this simple fact is of interest to diverse applications, including entanglement detection⁸⁻¹⁰ and quantum cryptography^{8,11,13}. Nevertheless, several fundamental questions are still left open. Notably, what quantum states of the system and memory can minimize or even eliminate the uncertainty completely? How much entanglement is required to achieve this goal?

In this paper we are interested in those quantum states that can eliminate the uncertainty completely, which are referred to as zero uncertainty states (ZUSs) henceforth. In contrast with the familiar minimum uncertainty states and intelligent states studied in the literature^{14–16}, our definition of ZUSs does not rely on a specific uncertainty measure, but has a clear operational interpretation. In particular, we determine all ZUSs with respect to any given set of nondegenerate observables on a finite-dimensional Hilbert space coupled with a quantum memory. We also determine the minimum entanglement required to construct any ZUS. It turns out all ZUSs are determined by a simple graph constructed from transition probabilities between eigenbases of the relevant observables. Moreover, all ZUSs are maximally entangled states (MESs), and vice versa, whenever this graph is connected. Notably, this is the case for a generic set of two or more observables, even if these observables are only weakly incompatible. Nevertheless, ZUSs and MESs are not necessarily pure states.

Our study establishes a simple and precise connection between zero uncertainty and maximum entanglement, which is independent of specific uncertainty and entanglement measures. Moreover, our approach applies to arbitrary sets of nondegenerate observables, in sharp contrast with most previous approaches, which are restricted to two observables or complementary observables. This work may shed light on the foundational studies of uncertainty relations, quantum entanglement, and quantum steering^{7,17–20}. Meanwhile, it is of direct interest to many tasks in quantum information processing, including remote state preparation^{21,22} and semi-device-independent quantum certification and verification^{18,23–26}.

RESULTS

Maximally entangled states

To establish our main results, first we need to better understand MESs. A bipartite state ρ on the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$ of dimension $d_A \times d_B$ is a MES if we can create every state on $\mathcal{H}_A \otimes \mathcal{H}_B$ from ρ by local operations and classical communication $(LOCC)^{27}$. This definition is independent of any specific entanglement measure and is thus quite appealing to the current study. When $d_A \leq d_B$, the state $|\Phi\rangle := \sum_{j=0}^{d_A-1} |jj\rangle / \sqrt{d_A}$ is a canonical example, where $\{|j\rangle\}_{j=0}^{d_A-1}$ and $\{|j\rangle\}_{j=0}^{d_B-1}$ are the computational bases of \mathcal{H}_A and \mathcal{H}_B , respectively. A MES is not necessarily pure, as clarified in the following lemma, essentially proved in ref. ²⁸; see the Supplementary Information for an independent proof.

Lemma 1 Let ρ be a bipartite state on $\mathcal{H}_A \otimes \mathcal{H}_B$ with $d_A \leq d_B$. Then the following statements are equivalent.

- 1. ρ is a MES.
- 2. $H(A|B)_{\rho} = -\log_2 d_A$.
- 3. $E_{\rm R}(\rho) = \log_2 d_{\rm A}$.
- 4. $E_{\rm F}(\rho) = \log_2 d_{\rm A}$.
- 5. ρ has a spectral decomposition $\rho = \sum_s \lambda_s |\Psi_s\rangle \langle \Psi_s|$ such that all $|\Psi_s\rangle$ are MESs, and $tr_A(|\Psi_s\rangle \langle \Psi_s|)$ have mutually orthogonal supports.

Here $H(A|B)_{\rho} = S(\rho) - S(\rho_B)$ is the conditional entropy of A given B, where $S(\rho)$ and $S(\rho_B)$ are the von Neumann entropies of ρ and $\rho_B := tr_A(\rho)$, respectively. $E_R(\rho)$ and $E_F(\rho)$ are the relative entropy of entanglement and entanglement of formation²⁷. By Lemma 1, all MESs on $\mathcal{H}_A \otimes \mathcal{H}_B$ are pure when $d_A \le d_B < 2d_A^{28}$. In general,

¹State Key Laboratory of Surface Physics and Department of Physics, Fudan University, Shanghai, China. ²Institute for Nanoelectronic Devices and Quantum Computing, Fudan University, Shanghai, China. ³Center for Field Theory and Particle Physics, Fudan University, Shanghai, China. ⁴Collaborative Innovation Center of Advanced Microstructures, Nanjing, China. ^{Semail:} zhuhuangjun@fudan.edu.cn

H. Zhu



Fig. 1 Connection between zero uncertainty and maximum entanglement in the uncertainty game. By performing suitable measurements (depending on the observables of Alice) on his quantum memory, Bob can better predict the measurement outcomes of Alice. When the set of observables of Alice is irreducible, Bob can predict these measurement outcomes with certainty iff his quantum memory is maximally entangled with Alice.

each MES is a convex mixture of pure MESs whose local supports for Bob are mutually orthogonal. Given a MES ρ on $\mathcal{H}_A \otimes \mathcal{H}_B$ with $d_A \leq d_{B'}$ let $\mathcal{H}_{B'}$ be the support of ρ_B . Then $\mathcal{H}_{B'}$ has a decomposition $\mathcal{H}_{B'} = \mathcal{H}_{B_1} \otimes \mathcal{H}_{B_2}$ with $\dim(\mathcal{H}_{B_1}) = d_A$ such that $\rho = |\Phi'\rangle\langle\Phi'| \otimes \tau$, where $|\Phi'\rangle$ is a pure MES in $\mathcal{H}_A \otimes \mathcal{H}_{B_1}$, and τ is a full-rank density operator on \mathcal{H}_{B_2} . So all MESs on $\mathcal{H}_A \otimes \mathcal{H}_B$ are equivalent under local operations of Bob.

Corollary 1 All MESs on $\mathcal{H}_A \otimes \mathcal{H}_B$ with $d_A \leq d_B$ can be turned into each other by local operations on \mathcal{H}_B . When $d_A \leq d_B < 2d_A$, all MESs are pure and can be turned into each other by unitary transformations on \mathcal{H}_B .

Zero uncertainty states

Consider the uncertainty game in which Alice can measure *m* nondegenerate von Neumann observables $\mathcal{O} = \{O_x\}_{x=1}^m$ on \mathcal{H}_A with uniform probabilities (generalization to nonuniform probabilities is straightforward), and Bob is asked to predict the measurement outcome given the specific observable chosen by Alice⁸. Let $\mathcal{B}_x = \{|\psi_{xk}\rangle\}_k$ be an orthonormal eigenbasis of O_x and $\mathcal{B} = \{\mathcal{B}_x\}_{x=1}^m$. Then predicting the outcome of O_x amounts to predicting the outcome of the projective measurement on the basis \mathcal{B}_x . When these observables are incompatible (do not commute with each other), in general Bob cannot predict the measurement outcome with certainty even if he knows the complete classical description of the system state as characterized by the density matrix ρ_A . In the case of two observables for example, the uncertainties of the measurement outcomes satisfy the Maassen-Uffink inequality²⁹,

$$H(O_1) + H(O_2) \ge \log_2(c^{-1}),$$
 (1)

where $H(O_1)$ and $H(O_2)$ are the Shannon entropies of the measurement outcomes of O_1 and O_2 , respectively, and $c = \max_{j,k} |\langle \psi_{1j} | \psi_{2k} \rangle|^2$.

The situation is different if Bob holds a quantum memory with Hilbert space \mathcal{H}_{B} and can create an entangled state ρ on the joint system $\mathcal{H}_{A} \otimes \mathcal{H}_{B}$, as illustrated in Fig. 1. Suppose Alice chooses the basis \mathcal{B}_{x} (observable O_{x}), then Bob can perform a generalized measurement characterized by a positive operator-valued measure (POVM) { Π_{xk} } on his subsystem \mathcal{H}_{B} , where Π_{xk} corresponds to guessing the outcome k given the measurement basis \mathcal{B}_{x} of Alice. The average success guessing probability reads $\sum_{x} p_{x}/m$ with

$$p_{x} = \sum_{k} \operatorname{tr} \left[\rho(|\psi_{xk}\rangle \langle \psi_{xk}| \otimes \Pi_{xk}) \right] = \sum_{k} \operatorname{tr} \left(\rho_{xk} \Pi_{xk} \right), \tag{2}$$

where $\rho_{xk} = \langle \psi_{xk} | \rho | \psi_{xk} \rangle$ are subnormalized reduced states of Bob. Note that p_x is also the probability that the POVM $\{\Pi_{xk}\}_k$ can successfully distinguish the ensemble of states

$$\mathscr{S}(\boldsymbol{\rho},\mathcal{B}_{\mathbf{x}}) = \{ \langle \boldsymbol{\psi} | \boldsymbol{\rho} | \boldsymbol{\psi} \rangle : | \boldsymbol{\psi} \rangle \in \mathcal{B}_{\mathbf{x}} \}.$$
(3)

The maximum of the average guessing probability over all POVMs can be determined by semidefinite programming, and this maximum is determined by the state ρ and the basis set \mathscr{B} (or the observable set \mathscr{O}) of Alice.

Given a set of observables $\mathcal{O} = \{O_x\}_{x=1}^m$ or bases $\mathscr{B} = \{\mathcal{B}_x\}_{x=1}^m$ for Alice, a joint state ρ of Alice and Bob is a ZUS if Bob can predict the measurement outcome of Alice with certainty by a suitable measurement depending on the choice of Alice. Given a ZUS, the guessing probability p_x for each measurement of Alice can attain the maximum 1, and the conditional entropy $H(O_x|B)$ is 0. In contrast with minimum uncertainty states and intelligent states^{14–16}, ZUSs not only minimize the uncertainty, but also eliminate the uncertainty completely. Moreover, here the definition is independent of any specific uncertainty measure.

To appreciate the significance of entanglement to constructing a ZUS, consider an example with two observables, in which case the uncertainty relation in Eq. (1) is modified as follows⁸,

$$H(O_1|B) + H(O_2|B) \ge \log_2(c^{-1}) + H(A|B)_{\rho}.$$
(4)

Here the conditional entropy $H(A|B)_{\rho}$ manifests the impact of entanglement in reducing the uncertainty. Interestingly, a variant of Eq. (4) may be interpreted as uncertainty-reality complementarity, which builds on an intimate connection between uncertainty (or rather certainty) and reality^{7,30–32}.

By Eq. (4), any ZUS ρ must satisfy the inequalities

$$E_{\mathsf{F}}(\rho) \ge E_{\mathsf{R}}(\rho) \ge -H(\mathsf{A}|\mathsf{B})_{\rho} \ge \log_2(c^{-1}),\tag{5}$$

where the second one is derived in ref. ³³ (cf. ref. ³⁴). Suppose O_1 and O_2 are complementary, so that \mathcal{B}_1 and \mathcal{B}_2 are mutually unbiased, which means $|\langle \psi_{1j} | \psi_{2k} \rangle|^2 = 1/d_A$ for all j, k^{35} . Then we have $c = 1/d_A$ and

$$E_{\mathsf{F}}(\rho) = E_{\mathsf{R}}(\rho) = -H(\mathsf{A}|\mathsf{B})_{\rho} = \log_2 d_{\mathsf{A}},\tag{6}$$

which implies that $d_B \ge d_A$ and ρ is a MES by Lemma 1, in which case ρ is indeed a ZUS. Unfortunately, this reasoning does not work in general. To address this problem, we need a completely different line of thinking.



Fig. 2 Transition graph of three mutually unbiased bases for a qubit, which corresponds to the eigenbases of the three Pauli matrices. Two vertices of the same color are associated with the two states in the same basis. This transition graph is connected, so the corresponding basis set is irreducible.

Key observations about ZUSs

Bob can predict the measurement outcome on the basis \mathcal{B}_x with certainty iff the ensemble $\mathscr{S}(\rho, \mathcal{B}_x)$ defined in Eq. (3) is perfectly distinguishable, that is, all states in $\mathscr{S}(\rho, \mathcal{B}_x)$ have mutually orthogonal supports. The state ρ is a ZUS with respect to $\mathscr{B} = \{\mathcal{B}_x\}_{x=1}^m$ iff each ensemble $\mathscr{S}(\rho, \mathcal{B}_x)$ is perfectly distinguishable. The following three propositions are simple corollaries of these observations.

Proposition 1 Suppose ρ is a ZUS, then any state supported in the support of ρ is a ZUS.

Proposition 2 Suppose ρ_1 and ρ_2 are two ZUSs on $\mathcal{H}_A \otimes \mathcal{H}_B$. If $\operatorname{tr}_A(\rho_1)$ and $\operatorname{tr}_A(\rho_2)$ have orthogonal supports, then any convex mixture of ρ_1 and ρ_2 is a ZUS.

Proposition 3 Suppose ρ is bipartite state on $\mathcal{H}_A \otimes \mathcal{H}_B$ and Λ is a completely positive and trace-preserving (CPTP) map (quantum channel) from system B to system \tilde{B} . Then ρ is a ZUS if $(1 \otimes \Lambda)(\rho)$ is.

Here Propositions 1 and 2 are tied to the fact that mixture of quantum states can only reduce distinguishability unless the reduced states of Bob have orthogonal supports. Proposition 3 follows from the simple fact that quantum operations cannot enhance distinguishability. Two states ρ_1 and ρ_2 on $\mathcal{H}_A \otimes \mathcal{H}_B$ are equivalent if they can be turned into each other by local operations on \mathcal{H}_B . In that case, ρ_1 is a ZUS with respect to \mathscr{B} iff ρ_2 is. Under these local operations, ZUSs divide into equivalent classes.

Transition graphs

To determine ZUSs with respect to a given basis set $\mathscr{B} = \{\mathcal{B}_x\}_{x=1}^m$ in \mathcal{H}_A , we first need to pinpoint a key property of the basis set. The transition graph $G(\mathscr{B})$ of \mathscr{B} is an *m*-partite graph with md_A vertices which are in one-to-one correspondence with the basis states (identical states in different bases correspond to different vertices). Two different vertices are adjacent iff the corresponding states are not orthogonal, that is, the transition probability between the two states is nonzero. The graph $G(\mathscr{B})$ encodes the incompatibility structure of the basis set \mathscr{B} , which is crucial to studying ZUSs and quantum verification, as we shall see later.

The basis set \mathscr{B} is irreducible if the transition graph $G(\mathscr{B})$ is connected, in which case the projectors onto basis states generate the whole operator algebra on \mathcal{H}_A . Any basis set composed of $m \ge 2$ mutually unbiased bases (or generic random bases) is irreducible since the transition graph is a complete *m*-partite graph, as illustrated in Fig. 2.

$$P_{a} = P_{a}(\mathscr{B}) = \sum_{|\psi\rangle \in \mathcal{B}_{x}^{a}} |\psi\rangle \langle \psi|, \quad r_{a} = \operatorname{tr}(\mathsf{P}_{\mathsf{a}}).$$
(7)

These definitions are independent of the choice of the basis index *x*. Denote by $\mathscr{P}(\mathscr{B}) := \{P_a(\mathscr{B})\}_{a=1}^g$ the set of component projectors, which are mutually orthogonal. In this way, \mathcal{H}_A decomposes into a direct sum of component subspaces $\mathcal{H}_{A,a}$. In addition, \mathcal{B}_x^a for x = 1, 2, ..., m can be regarded as bases in $\mathcal{H}_{A,a}$, and the basis set $\mathscr{B}^a := \{\mathcal{B}_x^a\}_{x=1}^m$ is irreducible for $\mathcal{H}_{A,a}$.

Connect ZUSs with MESs

Now we are ready to present our main results on ZUSs and MESs as illustrated in Fig. 1. First, we clarify when Bob can predict the outcome of one projective measurement of Alice. The following lemma proved in the Supplementary Information is a stepping stone to understanding ZUSs in the presence of a quantum memory.

Lemma 2 Suppose $\rho = |\Psi\rangle\langle\Psi|$ is a bipartite pure state on $\mathcal{H}_A \otimes \mathcal{H}_B$ and \mathcal{B} is an orthonormal basis for \mathcal{H}_A . Then the ensemble $\mathscr{S}(\rho, \mathcal{B})$ is perfectly distinguishable iff \mathcal{B} is an eigenbasis of $\rho_A = \operatorname{tr}_B(\rho)$.

Note that Bob can predict the measurement outcome of Alice on the basis \mathcal{B} with certainty iff the ensemble $\mathscr{S}(\rho, \mathcal{B})$ defined in Eq. (3) is perfectly distinguishable. By Lemma 2, this is the case iff ρ_A is diagonal with respect to the basis \mathcal{B} . Therefore, the pure state ρ is a ZUS with respect to a basis set \mathscr{B} iff ρ_A is diagonal with respect to each basis in \mathscr{B} . When \mathscr{B} is irreducible, it turns out only MESs can satisfy this condition. Based on this observation we can derive the following theorem as proved in the Supplementary Information.

Theorem 1 Suppose \mathscr{B} is an irreducible basis set in \mathcal{H}_A . Then a bipartite (pure or mixed) state ρ on $\mathcal{H}_A \otimes \mathcal{H}_B$ is a ZUS with respect to \mathscr{B} iff $d_B \ge d_A$ and ρ is a MES.

By Theorem 1 and Lemma 1, each ZUS with respect to \mathscr{B} is a tensor product of a pure MES and an ancillary state. In addition, to attain zero uncertainty, the measurements of Bob on the support of $\rho_{\rm B}$ are uniquely determined by the counterpart of Alice, as shown in Supplementary note E. All ZUSs with respect to \mathscr{B} can be turned into each other by local operations on $\mathcal{H}_{\rm B}$ and thus form a single equivalent class. If $d_{\rm A} \le d_{\rm B} < 2d_{\rm A}$, then all ZUSs are pure and can be turned into each other by unitary transformations on $\mathcal{H}_{\rm B}$. These results hold as long as the transition graph $G(\mathscr{B})$ is connected, even if \mathscr{B} consists of only two nearly identical bases, so that the corresponding observables are only weakly incompatible, as quantified by the commutator or incompatibility robustness^{36–38}.

Theorem 1 establishes a simple and precise connection between zero uncertainty and maximum entanglement, which is independent of specific uncertainty and entanglement measures. This connection offers a fresh perspective for understanding the uncertainty principle in the presence of a quantum memory⁸. It may also shed light on uncertainty-reality complementarity given the close relation between the notation of uncertainty and that of reality^{7,30–32}.

ZUSs with respect to reducible basis sets

Next, we determine ZUSs with respect to a reducible basis set \mathcal{B} .

Theorem 2 Suppose \mathscr{B} is a set of orthonormal bases in \mathcal{H}_A and has g irreducible components with component subspaces $\mathcal{H}_{A,ar}$ component projectors P_{ar} and component ranks r_a for a = 1, 2, ..., g. Let ρ be a bipartite state on $\mathcal{H}_A \otimes \mathcal{H}_B$ and $\rho_a = (P_a \otimes 1_B)\rho(P_a \otimes 1_B)$. Then ρ is a ZUS with respect to \mathscr{B} iff the following three conditions hold: $r_a \leq d_B$ whenever tr (ρ_a)>0; each ρ_a with tr (ρ_a)>0 is a (subnormalized) MES on $\mathcal{H}_{A,a} \otimes \mathcal{H}_B$; all tr $_A(\rho_a)$ have mutually orthogonal supports.

Theorem 2 follows from Theorem 1. Recall that the basis set \mathscr{B} can be regarded as a direct sum of irreducible basis sets \mathscr{B}^a defined on component subspaces $\mathcal{H}_{A,a}$. So ρ is a ZUS with respect to \mathscr{B} iff its restriction ρ_a on $\mathcal{H}_{A,a} \otimes \mathcal{H}_B$ is a ZUS with respect to \mathscr{B}^a and, in addition, all tr_A(ρ_a) have mutually orthogonal supports. Note that coherence between different component subspaces are useless to constructing ZUSs. In addition, the dimension d_B of \mathcal{H}_B must satisfy $d_B \geq r_{\min}$ in order to construct a ZUS, where $r_{\min} = \min_{1 \leq a \leq g} r_a$ is the minimum component rank. When the lower bound is saturated, every ZUS is a pure MES on $\mathcal{H}_{A,a} \otimes \mathcal{H}_B$, where $\mathcal{H}_{A,a}$ is a component subspace of dimension r_{\min} . Furthermore, r_{\min} determines the minimum entanglement required to construct a ZUS, as shown in the Methods section.

In the case of pure states, ZUSs admit a much simpler characterization, as shown in the following corollary.

Corollary 2 A bipartite pure state $|\Psi\rangle$ in $\mathcal{H}_A \otimes \mathcal{H}_B$ is a ZUS with respect to \mathscr{B} iff the reduced state ρ_A is a weighted sum of component projectors in $\mathscr{P}(\mathscr{B})$.

Corollary 2 is a special case of Theorem 2 and also follows from Lemma 2 and Supplementary Lemma 2. Here ρ_A is a weighted sum of component projectors iff ρ_A is diagonal with respect to each basis \mathcal{B} in \mathscr{B} (cf. Supplementary note C). As an implication of Corollary 2, the reduced state ρ_A of any (pure or mixed) ZUS ρ with respect to \mathscr{B} is a weighted sum of component projectors in $\mathscr{P}(\mathscr{B})$, given that any ZUS is a convex mixture of pure ZUSs. The equivalent classes of pure ZUSs are determined in the Methods section.

Applications to quantum certification and verification

Our results on ZUSs have immediate implications for the verification of MESs. Suppose Alice and Bob want to create the MES $|\Phi\rangle = \sum_{j=0}^{d_A-1} |jj\rangle / \sqrt{d_A}$ in this way: Bob first creates a MES in his lab and then sends one particle of the entangled pair to Alice via a quantum channel. To verify the resulting state ρ , they can perform tests based on correlated local projective measurements such that only the target state can pass all tests with certainty^{39–43}. Suppose Alice can perform projective measurements from the set $\mathscr{B} = \{\mathcal{B}_x\}_{x=1}^m$ in which \mathcal{B}_x is chosen with probability $\mu_x > 0$. For each choice \mathcal{B}_x , she asks Bob to perform the measurement on the conjugate basis \mathcal{B}_x^* and return the outcome. The test is passed if Bob and Alice obtain the same outcome⁴¹.

If Bob is honest, then the average probability that ρ passes each test is tr ($\rho\Omega$), where $\Omega = \sum_{x=1}^{m} \mu_x P(\mathcal{B}_x)^{41}$ is known as the verification operator and

$$P(\mathcal{B}_{x}) := \sum_{|\psi\rangle \in \mathcal{B}_{x}} |\psi\rangle \langle \psi| \otimes |\psi^{*}\rangle \langle \psi^{*}|$$
(8)

is a test projector. Note that $|\Phi\rangle$ is an eigenstate of $P(\mathcal{B}_x)$ and Ω with eigenvalue 1 and so can pass each test with certainty. In addition, $|\Phi\rangle$ can be reliably verified by this protocol iff the maximum eigenvalue of Ω is nondegenerate, that is, the pass eigenspace of Ω has dimension 1^{40-43} . This is the case iff the basis set \mathscr{B} is irreducible by the following theorem proved in the Supplementary Information.

Theorem 3 Suppose $\mathscr{B} = \{\mathcal{B}_x\}_{x=1}^m$ is a set of orthonormal bases in \mathcal{H}_{A_r} and $\Omega = \sum_{x=1}^m \mu_x P(\mathcal{B}_x)$ with $\mu_x > 0$ and $\sum_{x=1}^m \mu_x = 1$. Then the degeneracy of the maximum eigenvalue 1 of Ω equals the Next, suppose Bob is not honest. Then Alice cannot distinguish states that are equivalent under the local operations of Bob. Nevertheless, she can still verify the MES $|\Phi\rangle$ up to equivalence. Thanks to Theorem 1, the uncertainty game described before actually provides a verification protocol whenever the basis set \mathscr{B} of Alice is irreducible. Note that Bob can pass each test (guess each measurement outcome) of Alice with certainty only if the state ρ prepared is a MES. Surprisingly, the requirement on the measurement bases of Alice remains the same when Bob becomes dishonest. In addition, the measurements of Bob required to attain the maximum guessing probability are essentially uniquely determined by the counterpart of Alice. These results are of interest to semi-device-independent quantum certification and verification^{18,23–26}

Implications for quantum steering

Our study also has implications for Einstein-Podolsky-Rosen steering or quantum steering^{7,17–20}, which is clear if we interchange the measurement order in the above verification protocol. In each test Alice asks Bob to perform the measurement on the basis \mathcal{B}_x^* with probability $\mu_x > 0$ for x = 1, 2, ..., m and return the outcome. Then Alice performs the projective measurement on $\mathcal{B}_x \in \mathscr{B}$, and the test is passed if she obtains the same outcome as Bob. Alternatively, Alice can choose the two-outcome POVM $\{|\psi_{xk}\rangle\langle\psi_{xk}|, 1_A - |\psi_{xk}\rangle\langle\psi_{xk}|\}$ if Bob obtains outcome *k*. Suppose Alice and Bob share the state ρ and Bob performs the POVM $\{\Pi_{xk}\}_k$ instead of the projective measurement on \mathcal{B}_x^* . Then the probability that Bob passes the test reads

$$\sum_{k} \langle \psi_{xk} | \sigma_{xk} | \psi_{xk} \rangle, \quad \sigma_{xk} = \operatorname{tr}_{\mathsf{B}}[\rho(\mathbf{1}_{\mathsf{A}} \otimes \Pi_{xk})], \tag{9}$$

which is a variant of Eq. (2). The subnormalized states σ_{xk} satisfy the normalization condition $\sum_k \sigma_{xk} = \rho_A$ and form an *ensemble* of ρ_A for each *x*. The collection of ensembles $\{\{\sigma_{xk}\}_k\}_x$ is known as an *assemblage*^{19,20,44}. If Bob is honest, then the assemblage generated is $\{\{|\psi_{xk}\rangle\langle\psi_{xk}|/d_A\}_k\}_x$. When \mathscr{B} is irreducible, it turns out only this assemblage can pass each test with certainty, as shown in the following lemma and proved in the Supplementary Information.

Lemma 3 Suppose $\mathscr{B} = \{\mathcal{B}_x\}_{x=1}^m$ with $\mathcal{B}_x = \{|\psi_{xk}\rangle\}_k$ is an irreducible set of orthonormal bases in \mathcal{H}_A . Suppose $\{\{\sigma_{xk}\}_k\}_x$ is an assemblage for ρ_A that satisfies $\sum_k \langle \psi_{xk} | \sigma_{xk} | \psi_{xk} \rangle = 1$ for each x. Then ρ_A is completely mixed, and $\sigma_{xk} = |\psi_{xk}\rangle \langle \psi_{xk}|/d_A$ for each x and k.

Here the condition $\sum_{k} \langle \psi_{xk} | \sigma_{xk} | \psi_{xk} \rangle = 1$ means the assemblage $\{\{\sigma_{xk}\}_k\}_x$ can pass each test of Alice with certainty. By virtue of Theorem 1, we can further show that the assemblage $\{\{|\psi_{xk}\rangle\langle\psi_{xk}|/d_A\}_k\}_x$ can only be generated by a MES, as stated in the following theorem and proved in the Supplementary Information.

Theorem 4 Given the basis set \mathscr{B} in Lemma 3, suppose ρ is a bipartite state on $\mathcal{H}_A \otimes \mathcal{H}_B$ that can generate the assemblage $\{\{|\psi_{xk}\rangle\langle\psi_{xk}|/d_A\}_k\}_x$ under the measurements of Bob. Then $d_B \ge d_{A'}$ and ρ is a MES and a ZUS with respect to \mathscr{B} .

Thanks to Lemma 3 and Theorem 4, the tests of Alice can verify the assemblage $\{\{|\psi_{xk}\rangle\langle\psi_{xk}|/d_A\}_k\}_{x'}$ which in turn can verify the MES whenever \mathscr{B} is irreducible. In addition, Theorem 4 offers a general recipe for constructing assemblages that are characteristic of MESs. These results establish intimate connections between uncertainty relations, quantum entanglement, and quantum steering, which are of intrinsic interest to foundational studies. Meanwhile, these results are instructive to studying remote state preparation^{21,22} and semi-device-independent self testing^{18,23-26}.

DISCUSSION

ZUSs in the presence of a quantum memory are particular quantum states that can eliminate uncertainties of incompatible von Neumann observables once assisted by suitable measurements on the memory. In this work, we determined all ZUSs with respect to any given set of nondegenerate observables in the presence of a quantum memory. To achieve this goal we introduced several useful tools that apply to an arbitrary set of observables, in sharp contrast with most previous approaches, which only apply to two observables or complementary observables. In addition, we determined the minimum entanglement required to construct a ZUS. Our study shows that all ZUSs are MESs for a generic set of two or more observables even if these observables are only weakly incompatible. In this way, we establish a simple and precise connection between ZUSs and MESs. This connection may shed light on the uncertainty principle in the presence of a quantum memory. It is of intrinsic interest to studying a number of fascinating topics, including the uncertainty principle, quantum entanglement, and quantum steering. Moreover, it has direct applications in semi-device-independent quantum certification and verification, which is currently an active research field.

METHODS

ZUSs with least entanglement

Here we determine the minimum entanglement required to construct a ZUS, following the premises and notations in Theorem 2.

Given the basis set \mathscr{B} in Theorem 2, define $\Lambda_{\mathscr{B}}$ as the CPTP map acting on quantum states on $\mathcal{H}_A\otimes\mathcal{H}_B$ that removes coherence between different component subspaces, that is,

$$\Lambda_{\mathscr{B}}(\rho) = \sum_{a} (P_a \otimes 1_{\mathsf{B}})\rho(P_a \otimes 1_{\mathsf{B}}) = \sum_{a} \rho_a = \bigoplus_{a} \rho_a, \tag{10}$$

where $\rho_a = (P_a \otimes 1_B)\rho(P_a \otimes 1_B)$ and P_a are component projectors defined in Eq. (7). Note that the map $\Lambda_{\mathscr{B}}$ can be realized by LOCC. In addition, ρ is a ZUS with respect to \mathscr{B} iff $\rho_{\mathscr{B}} := \Lambda_{\mathscr{B}}(\rho)$ is. When ρ is a ZUS, $\rho_{\mathscr{B}}$ is a direct sum of subnormalized MESs ρ_a according to Theorem 2.

The component vector is defined as

$$\mathbf{q}(\boldsymbol{\rho},\mathscr{B}) := (q_a)_a, \quad q_a := \operatorname{tr}\left[\boldsymbol{\rho}(\mathsf{P}_{\mathsf{a}} \otimes \mathsf{1}_{\mathsf{B}})\right] = \operatorname{tr}\left(\boldsymbol{\rho}_{\mathsf{a}}\right); \tag{11}$$

it is invariant under the local operations of Bob and is very useful to studying the entanglement properties and equivalent classes of ZUSs. Note that $\rho_{\mathscr{B}}$ and ρ share the same component vector. The following theorem is proved in the Supplementary Information.

Theorem 5 Suppose *E* is an entanglement measure, then any ZUS ρ with component vector $\mathbf{q}(\rho, \mathscr{B}) = (q_a)_a$ satisfies

$$E(\rho) \ge E(\rho_{\mathscr{B}}) \ge \sum_{a} q_{a} E(|\Phi(r_{a})\rangle) \ge E(|\Phi(r_{\min})\rangle), \tag{12}$$

where $|\Phi(r_a)\rangle$ is a MES of Schmidt rank r_a . The second inequality in Eq. (12) is saturated if E is a convex entanglement measure.

Here $r_a = \text{tr}(P_a)$ is the component rank defined in Eq. (7), and $r_{\min} = \min_{1 \le a \le g} r_a$ is the minimum component rank. Theorem 5 applies to any entanglement measure *E* that is monotonic under selective and nonselective LOCC. In addition, the lower bounds for $E(\rho)$ only depend on the values of the measure *E* at pure MESs.

When $\rho_{\mathscr{R}} \neq \rho$, the inequality $E(\rho) \ge E(\rho_{\mathscr{R}})$ in Eq. (12) is strict for many entanglement measures, including the entanglement of formation, as shown in Corollary 5 below. To determine least entangled ZUSs, we can assume the condition $\rho = \rho_{\mathscr{R}}$, so ρ has no coherence between different component subspaces. Such a ZUS is called economical. In addition, the third inequality in Eq. (12) is usually strict unless $q_a = 0$ when $r_a > r_{\min}$ (cf. Corollary 6 below). An economical ZUS ρ with $q_a = 0$ for all $r_a > r_{\min}$ is called a *ZUS* with least entanglement (ZUSLE) since it can saturate the ultimate lower bound in Eq. (12) for every convex entanglement measure. Such a state can be expressed as follows,

$$\rho = \rho_{\mathscr{B}} = \sum_{a|r_a = r_{\min}} \rho_a = \bigoplus_{a|r_a = r_{\min}} \rho_a.$$
(13)

It has no coherence between different component subspaces, and its local support for Alice can only contain component subspaces with the

minimum component rank r_{min} . The operational significances of ZUSLEs can be summarized as follows.

Corollary 3 Every ZUS on $\mathcal{H}_A \otimes \mathcal{H}_B$ with respect to \mathscr{B} can be turned into a ZUSLE by LOCC. In addition, all ZUSLEs can be turned into each other by LOCC.

Corollary 4 A ZUS on $\mathcal{H}_A \otimes \mathcal{H}_B$ with respect to \mathscr{B} is a ZUSLE iff it can be created from $|\Phi(r_{min})\rangle$ by LOCC.

Corollary 3 follows from Theorem 2 and Corollary 1. Corollary 4 follows from Corollary 3 and Corollary 6 below. This operational characterization of ZUSLEs is independent of specific entanglement measures, which complements the operational definition of ZUSs in the main text.

Corollary 5 Any ZUS ρ with component vector $\mathbf{q}(\rho, \mathscr{B}) = (q_a)_a$ satisfies $E_{\mathsf{F}}(\rho) \geq \sum_a q_a \log_2 r_a$. The lower bound is saturated iff $\rho = \rho_{\mathscr{B}}$.

Corollary 6 Any ZUS ρ with respect to \mathscr{B} satisfies $E_F(\rho) \ge \log_2 r_{\min}$, which is saturated iff ρ is a ZUSLE.

Corollary 5 is proved in the Supplementary Information. Corollary 6 follows from Corollary 5 (cf. Theorem 5). When \mathscr{B} is irreducible, the bound $E_{\rm F}(\rho) \geq \sum_a q_a \log_2 r_a$ reduces to $E_{\rm F}(\rho) \geq \log_2 d_{\rm A}$, which is expected in view of Theorem 1 and Lemma 1. In general, the lower bound may be seen as a weighted average of bounds associated with individual irreducible components of \mathscr{B} . Incidentally, the bounds in Corollaries 5 and 6 still hold if $E_{\rm F}$ is replaced by any entanglement measure that coincides with $E_{\rm F}$ on pure states, such as the relative entropy of entanglement²⁷.

Equivalent classes of ZUSs

Here we clarify the equivalent classes of ZUSs under the local operations of Bob. Suppose ρ is a ZUS with respect to \mathscr{B} and has a component vector $\mathbf{q}(\rho,\mathscr{B}) = (q_a)_a$. According to Corollary 2, (cf. Theorem 2, Lemma 1, and Corollary 1), ρ_A is a weighted sum of component projectors,

$$\rho_{\mathsf{A}} = \sum_{a} \frac{q_{a} P_{a}}{r_{a}}.$$
(14)

Two ZUSs have the same reduced state and thus same measurement statistics for Alice iff they have the same component vector. So the equivalent classes of pure ZUSs are completely characterized by component vectors.

Corollary 7 Two pure ZUSs with respect to \mathcal{B} are equivalent iff they have the same component vector.

Given a ZUS ρ with respect to the basis set \mathscr{B} , denote by $\mathcal{H}_{B,a}$ the support of tr_A(ρ_a) and Q_a the corresponding projector; then Q_a and Q_b are orthogonal whenever $a \neq b$ by Theorem 2. In addition, we have

$$\rho_a = (\mathbf{1}_{\mathsf{A}} \otimes \mathbf{Q}_a)\rho(\mathbf{1}_{\mathsf{A}} \otimes \mathbf{Q}_a),\tag{15}$$

$$\rho_{\mathscr{B}} = \sum_{a} (\mathbf{1}_{\mathsf{A}} \otimes Q_{a}) \rho(\mathbf{1}_{\mathsf{A}} \otimes Q_{a}).$$
(16)

So ρ can be turned into $\rho_{\mathscr{R}}$ by local operations of Bob. Thanks to Corollary 1, $\rho_{\mathscr{R}}$ can further be turned into a direct sum of pure MESs of the form $\bigoplus_a q_a |\Phi_a\rangle \langle \Phi_a|$, where $|\Phi_a\rangle$ is a normalized MES in $\mathcal{H}_{A,a} \otimes \mathcal{H}_{B,a}$ (a product state when $r_a = 1$). These observations lead to the following corollary, which complements Corollary 7.

Corollary 8 Every ZUS on $\mathcal{H}_A \otimes \mathcal{H}_B$ with respect to \mathscr{B} can be turned into an economical ZUS with the same component vector by local operations of Bob. Two economical ZUSs are equivalent iff they have the same component vector.

Thanks to Corollary 8, equivalent classes of economical ZUSs with respect to \mathcal{B} are in one-to-one correspondence with component vectors, which form a probability simplex of dimension g - 1, where g is the number of irreducible components of \mathcal{B} . In particular, two ZUSLEs are equivalent iff they have the same component vector. If there is only one component subspace of dimension r_{\min} , then all ZUSLEs are equivalent.

DATA AVAILABILITY

No data set was generated or analyzed in the current study.

CODE AVAILABILITY

No code was generated or analyzed in the current study.

Received: 15 July 2020; Accepted: 22 January 2021; Published online: 08 March 2021

-

REFERENCES

- Heisenberg, W. Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik. Z. Phys. 43, 172 (1927).
- Busch, P., Lahti, P. & Werner, R. F. Colloquium: quantum root-mean-square error and measurement uncertainty relations. *Rev. Mod. Phys.* 86, 1261–1281 (2014).
- Coles, P. J., Berta, M., Tomamichel, M. & Wehner, S. Entropic uncertainty relations and their applications. *Rev. Mod. Phys.* 89, 015002 (2017).
- Werner, R. F. & Farrelly, T. Uncertainty from Heisenberg to today. Found. Phys. 49, 460–491 (2019).
- Kennard, E. H. Zur Quantenmechanik einfacher Bewegungstypen. Z. Phys. 44, 326–352 (1927).
- 6. Robertson, H. P. The uncertainty principle. Phys. Rev. 34, 163-164 (1929).
- Einstein, A., Podolsky, B. & Rosen, N. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.* 47, 777 (1935).
- 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).
- Li, C.-F., Xu, J.-S., Xu, X.-Y., Li, K. & Guo, G.-C. Experimental investigation of the entanglement-assisted entropic uncertainty principle. *Nat. Phys.* 7, 752–756 (2011).
- Prevedel, R., Hamel, D. R., Colbeck, R., Fisher, K. & Resch, K. J. Experimental investigation of the uncertainty principle in the presence of quantum memory and its application to witnessing entanglement. *Nat. Phys.* 7, 757–761 (2011).
- Tomamichel, M. & Renner, R. Uncertainty relation for smooth entropies. *Phys. Rev. Lett.* **106**, 110506 (2011).
- Coles, P. J., Colbeck, R., Yu, L. & Zwolak, M. Uncertainty relations from simple entropic properties. *Phys. Rev. Lett.* **108**, 210405 (2012).
- Tomamichel, M., Lim, C. C. W., Gisin, N. & Renner, R. Tight finite-key analysis for quantum cryptography. *Nat. Commun.* 3, 634 (2012).
- 14. Stoler, D. Equivalence classes of minimum uncertainty packets. *Phys. Rev. D* 1, 3217–3219 (1970).
- Hillery, M. & Mlodinow, L. Interferometers and minimum-uncertainty states. *Phys. Rev. A* 48, 1548–1558 (1993).
- Aragone, C., Chalbaud, E. & Salamó, S. On intelligent spin states. J. Math. Phys. 17, 1963–1971 (1976).
- Wiseman, H. M., Jones, S. J. & Doherty, A. C. Steering, entanglement, nonlocality, and the Einstein-Podolsky-Rosen paradox. *Phys. Rev. Lett.* 98, 140402 (2007).
- Šupić, I. & Hoban, M. J. Self-testing through EPR-steering. N. J. Phys. 18, 075006 (2016).
- Cavalcanti, D. & Skrzypczyk, P. Quantum steering: a review with focus on semidefinite programming. *Rep. Prog. Phys.* 80, 024001 (2017).
- Uola, R., Costa, A. C. S., Nguyen, H. C. & Gühne, O. Quantum steering. *Rev. Mod. Phys.* 92, 015001 (2020).
- 21. Bennett, C. H. et al. Remote state preparation. Phys. Rev. Lett. 87, 077902 (2001).
- Berry, D. W. & Sanders, B. C. Optimal remote state preparation. *Phys. Rev. Lett.* 90, 057901 (2003).
- Mayers, D. & Yao, A. Self testing quantum apparatus. *Quantum Info Comput.* 4, 273–286 (2004).
- McCutcheon, W. et al. Experimental verification of multipartite entanglement in quantum networks. *Nat. Commun.* 7, 13251 (2016).
- Šupić, I. & Bowles, J. Self-testing of quantum systems: a review. Quantum 4, 337 (2020).
- Eisert, J. et al. Quantum certification and benchmarking. Nat. Rev. Phys. 2, 382–390 (2020).
- Horodecki, R., Horodecki, P., Horodecki, M. & Horodecki, K. Quantum entanglement. *Rev. Mod. Phys.* 81, 865 (2009).
- Li, Z.-G., Zhao, M.-J., Fei, S.-M., Fan, H. & Liu, W. M. Mixed maximally entangled states. *Quantum Inf. Comput.* 12, 63 (2012).
- Maassen, H. & Uffink, J. B. M. Generalized entropic uncertainty relations. *Phys. Rev. Lett.* 60, 1103–1106 (1988).
- Bilobran, A. L. O. & Angelo, R. M. A measure of physical reality. *Europhys. Lett.* 112, 40005 (2015).
- Dieguez, P. R. & Angelo, R. M. Information-reality complementarity: the role of measurements and quantum reference frames. *Phys. Rev. A* 97, 022107 (2018).
- Rudnicki, Ł. Uncertainty-reality complementarity and entropic uncertainty relations. J. Phys. A: Math. Theor. 51, 504001 (2018).
- Plenio, M. B., Virmani, S. & Papadopoulos, P. Operator monotones, the reduction criterion and the relative entropy. J. Phys. A: Math. Gen. 33, L193 (2000).

- Zhu, H., Hayashi, M. & Chen, L. Coherence and entanglement measures based on Rényi relative entropies. J. Phys. A: Math. Theor. 50, 475303 (2017).
- Durt, T., Englert, B.-G., Bengtsson, I. & Życzkowski, K. On mutually unbiased bases. Int. J. Quantum Inf. 08, 535 (2010).
- Heinosaari, T., Kiukas, J. & Reitzner, D. Noise robustness of the incompatibility of quantum measurements. *Phys. Rev. A* 92, 022115 (2015).
- Haapasalo, E. Robustness of incompatibility for quantum devices. J. Phys. A: Math. Theor. 48, 255303 (2015).
- Uola, R., Budroni, C., Gühne, O. & Pellonpää, J.-P. One-to-one mapping between steering and joint measurability problems. *Phys. Rev. Lett.* 115, 230402 (2015).
- Hayashi, M., Matsumoto, K. & Tsuda, Y. A study of LOCC-detection of a maximally entangled state using hypothesis testing. J. Phys. A: Math. Gen. 39, 14427 (2006).
- Pallister, S., Linden, N. & Montanaro, A. Optimal verification of entangled states with local measurements. *Phys. Rev. Lett.* **120**, 170502 (2018).
- Zhu, H. & Hayashi, M. Optimal verification and fidelity estimation of maximally entangled states. *Phys. Rev. A* **99**, 052346 (2019).
- Zhu, H. & Hayashi, M. Efficient verification of pure quantum states in the adversarial scenario. *Phys. Rev. Lett.* **123**, 260504 (2019).
- Zhu, H. & Hayashi, M. General framework for verifying pure quantum states in the adversarial scenario. *Phys. Rev. A* **100**, 062335 (2019).
- Pusey, M. F. Negativity and steering: a stronger Peres conjecture. *Phys. Rev. A* 88, 032313 (2013).

ACKNOWLEDGEMENTS

This work is supported by the National Natural Science Foundation of China (Grant No. 11875110) and Shanghai Municipal Science and Technology Major Project (Grant No. 2019SHZDZX01).

AUTHOR CONTRIBUTIONS

H.Z. proposed this project, derived all the results, and wrote the paper.

COMPETING INTERESTS

The author declares no competing interests.

ADDITIONAL INFORMATION

Supplementary information The online version contains supplementary material available at https://doi.org/10.1038/s41534-021-00384-4.

Correspondence and requests for materials should be addressed to H.Z.

Reprints and permission 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 license, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this license, visit http://creativecommons. org/licenses/by/4.0/.

© The Author(s) 2021