Hiding and masking quantum information in complex and real quantum mechanics

Huangjun Zhu ◉*

State Key Laboratory of Surface Physics and Department of Physics, Fudan University, Shanghai 200433, China;
Institute for Nanoelectronic Devices and Quantum Computing, Fudan University, Shanghai 200433, China;
and Center for Field Theory and Particle Physics, Fudan University, Shanghai 200433, China

Classical information can be completely hidden in the correlations of bipartite quantum systems. However, it is impossible to hide or mask all quantum information according to the no-hiding and no-masking theorems derived recently. Here we show that any set of informationally complete quantum states is neither hidable nor maskable, thereby strengthening the no-hiding and no-masking theorems known before. Then, by virtue of Hurwitz-Radon matrices (representations of the Clifford algebra), we show that information about real quantum states can be completely hidden in the correlations, although the minimum dimension of the composite Hilbert space required increases exponentially with the dimension of the original Hilbert space. Moreover, the set of real quantum states is a maximal maskable set within quantum theory and has a surprising connection with maximally entangled states. These results offer valuable insight on the potential and limit of hiding and masking quantum information, which are of intrinsic interest to a number of active research areas.

I. INTRODUCTION

Hiding information in correlations is a simple way of realizing secret sharing [1,2], which is a primitive to cryptography and secure multiparty computation. In the quantum world, a similar idea is of interest to a wide spectrum of research topics, including but not limited to quantum secret sharing [3–5], quantum communication, information scrambling, and the black-hole information paradox [6–9]. However, it is impossible to hide or mask all quantum information in correlations according to the no-hiding theorem [10] and no-masking theorem [11] derived recently, in sharp contrast with classical information. These no-go theorems are reminiscent of the no-cloning theorem [12–14] and no-broadcasting theorem [15], which play crucial roles in quantum cryptography. On the other hand, little is known about hiding or masking quantum information in restricted sets of quantum states [16–18]. An example of special interest is the set of real quantum states as represented by real density matrices [19–23], which is the starting point of the resource theory of imaginarity [24,25].

Here we show that it is impossible to hide or mask any set of quantum states that is *informationally complete* (IC), thereby strengthening the no-hiding and no-masking theorems and establishing an information theoretical underpinning of these no-go results. This conclusion can serve as the common starting point for deriving and strengthening a number of re-

sults on quantum information masking. As implications, a set of qubit states is hidable or maskable iff the corresponding set of Bloch vectors is contained in a disk [11,16,17]. In addition, it is impossible to hide or mask any set of quantum states that has a nonzero measure; previously, quite restrictive assumptions are required to derive a similar result [26]. Furthermore, it is impossible to hide or mask any set of quantum states that can form a (weighted) 2-design.

By virtue of *Hurwitz-Radon* (HR) matrices [27–29], we further show that information about real quantum states can be completely hidden in the correlations. In addition, we determine the minimum dimension and entanglement cost required to achieve this task. It turns out the minimum dimension increases exponentially with the dimension of the original Hilbert space. Moreover, the set of real quantum sates is a maximal maskable set within quantum theory. Meanwhile, there is a simple connection between the concurrence [30–32] of the output state of any masker for real quantum states and the robustness of imaginarity of the input state [24,25]. Our study offers valuable insight on the potential and limit of hiding and masking quantum information. It may shed light on a number of active research areas, including quantum secret sharing [3–5], information scrambling, black-hole information paradox [6–9], resource theory of imaginarity [24,25], and foundational studies on quantum mechanics [33–35].

The rest of this paper is organized as follows. In Sec. II, we review the basic ideas of hiding and masking quantum information and introduce the concepts of masking spectrum, masking purity, entanglement of masking, and maximal maskable sets. In Sec. III, we prove that it is impossible to hide or mask any set of quantum states that is IC. In Sec. IV, we discuss the properties and construction of HR matrices. In Sec. V, we prove that the set of real quantum states is maskable and is a maximal maskable set. In Sec. VI, we construct a hidable
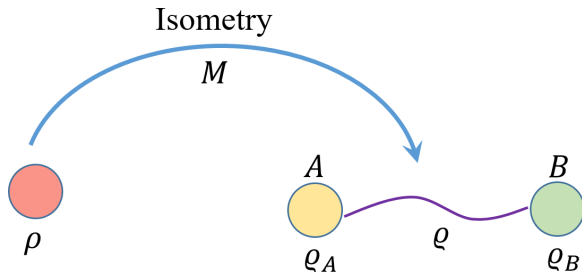
---

*zhuhuangjun@fudan.edu.cn

FIG. 1. Hiding and masking of quantum information. In the former case, ϱ_A is independent of ρ (in a given set $\mathscr{S}$); in the latter case, both ϱ_A and ϱ_B are independent of ρ.

set that is not maskable. In Sec. VII, we clarify the relation between real states and phase-parameterized states. Section VIII summarizes this paper. To streamline the presentation, most technical proofs are relegated to the Appendix.

II. HIDING AND MASKING QUANTUM INFORMATION

Let $\mathcal{H}$ be a d-dimensional Hilbert space with $d \geqslant 2$ and the computational basis $\{|j\rangle\}_{j=0}^{d-1}$. Denote by $\mathscr{D}(\mathcal{H})$ the set of all quantum states (represented by density matrices) on $\mathcal{H}$ and by $\mathscr{P}(\mathcal{H})$ the set of all pure states (represented by rank-1 projectors). Denote by $\mathscr{D}^{\mathrm{R}}(\mathcal{H})$ the set of real quantum states (represented by real density matrices with respect to the computational basis) and by $\mathscr{P}^{\mathrm{R}}(\mathcal{H})$ the set of real pure states.

Let M be an isometry from $\mathcal{H}$ to a bipartite Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$ of dimension $d_A \times d_B$. Let $\rho \in \mathscr{D}(\mathcal{H})$,

$$\varrho = M(\rho) := M\rho M^{\dagger}, \quad \varrho_A = \mathrm{tr}_B(\varrho), \quad \varrho_B = \mathrm{tr}_A(\varrho). \quad (1)$$

Given $\mathscr{S} \subseteq \mathscr{D}(\mathcal{H})$, define

$$M(\mathscr{S}) := M\mathscr{S}M^{\dagger} = \{\varrho | \rho \in \mathscr{S}\}. \quad (2)$$

If the reduced state ϱ_A is independent of ρ in $\mathscr{S}$, then M can hide the information of quantum states in the set $\mathscr{S}$ from subsystem A (cf. Fig. 1) and is called a *partial masker* (here we only consider partial maskers for subsystem A). So it is natural to expect that the information about the original states spreads over the correlations. However, this possibility is ruled by the no-hiding theorem when $\mathscr{S} = \mathscr{D}(\mathcal{H})$ or $\mathscr{S} = \mathscr{P}(\mathcal{H})$. In this case, any partial masker can only hide the information in a trivial way by transferring the information to another subsystem [10]. This surprising fact has implications for many active research topics, including the black-hole information paradox. However, little is known about this issue when $\mathscr{S}$ is a smaller subset.

The set $\mathscr{S}$ is *hidable* if it consists of only one quantum state or if there exists a nontrivial partial masker. Otherwise, the set $\mathscr{S}$ is *antiscrambling*. In the latter case, $\mathscr{S}$ contains at least two distinct quantum states and every partial masker $M : \mathcal{H} \mapsto \mathcal{H}_A \otimes \mathcal{H}_B$ for $\mathscr{S}$ is trivial in this sense: there exists a subspace $\mathcal{H}_B' = \mathcal{H}_{B_1} \otimes \mathcal{H}_{B_2}$ in $\mathcal{H}_B$ such that

$$M(\rho) = \varrho_{AB_1} \otimes \varrho_{B_2} \quad \forall \rho \in \mathscr{S}, \quad (3)$$

where ϱ_{AB_1} is a fixed density matrix on $\mathcal{H}_A \otimes \mathcal{H}_{B_1}$, which is independent of ρ in $\mathscr{S}$, while ϱ_{B_2} is a density matrix on $\mathcal{H}_{B_2}$ that depends on ρ. In the current language, the no-hiding theorem [10] states that $\mathscr{P}(\mathcal{H})$ and $\mathscr{D}(\mathcal{H})$ are antiscrambling.

By contrast, M can *mask* the set $\mathscr{S}$ if both ϱ_A and ϱ_B are independent of ρ (cf. Fig. 1); that is,

$$\mathrm{tr}_B[M(\rho)] = \tau_A, \quad \mathrm{tr}_A[M(\rho)] = \tau_B \quad \forall \rho \in \mathscr{S}, \quad (4)$$

where τ_A and τ_B are fixed density matrices and are referred to as the common reduced density matrices. In this case, M is called a *masker* for $\mathscr{S}$, and $\mathscr{S}$ is *maskable*. Note that the masker M can hide the information from both A and B, so all information is hidden in the correlations. Meanwhile, this masker offers a (2,2) threshold scheme for quantum secret sharing [4]. A maskable set $\mathscr{S}$ is *maximal* if it is not contained in any other maskable set in $\mathscr{D}(\mathcal{H})$. When $\mathscr{S} \subseteq \mathscr{D}^{\mathrm{R}}(\mathcal{H})$, the masker M is called a real masker if $M(\mathscr{S}) \subseteq \mathscr{D}^{\mathrm{R}}(\mathcal{H}_A \otimes \mathcal{H}_B)$.

The *masking spectrum* of M is defined as the nonzero spectrum of τ_A or τ_B, assuming that $\mathscr{S}$ contains at least one pure state, so that τ_A and τ_B have the same nonzero spectrum. The *masking purity* $\wp$ of M refers to the purity of τ_A or τ_B, that is,

$$\wp := \mathrm{tr}(\tau_A^2) = \mathrm{tr}(\tau_B^2). \quad (5)$$

Given a bipartite entanglement monotone E [36], the *entanglement of masking* of $\mathscr{S}$ is defined as

$$E(\mathscr{S}) := \min_M E(\mathscr{S}, M), \quad E(\mathscr{S}, M) := \max_{\rho \in \mathscr{S}} E(M(\rho)), \quad (6)$$

where the minimization is over all maskers M for $\mathscr{S}$. The entanglement of masking associated with real maskers can be defined in a similar way and is denoted by $E^{\mathrm{R}}(\mathscr{S})$. The following lemma is proved in Appendix A.

Lemma 1. Suppose $\mathscr{S}$ contains a pure state ρ_0 and M is a masker for $\mathscr{S}$. Then $E(\mathscr{S}, M) = E(M(\rho_0))$ for any entanglement monotone E.

If there exists no masker for $\mathscr{S}$, then $\mathscr{S}$ is not maskable. By Ref. [11], the sets $\mathscr{P}(\mathcal{H})$ and $\mathscr{D}(\mathcal{H})$ are not maskable. This no-masking theorem also follows from the no-hiding theorem [10]; note that a maskable set is hidable (not antiscrambling) by definition, and an antiscrambling set is not maskable. Nevertheless, a maskable set can contain infinite nonorthogonal quantum states. In particular, any set of phase-parameterized states is maskable [11] (cf. Sec. VII). In addition, any set of commuting density matrices is maskable [18] since these density matrices can be expressed as convex mixtures of pure states in an orthonormal basis and so can be masked using a generalized Bell basis. Together with Ref. [15], this fact implies that any set of quantum states that can be broadcast is maskable, as illustrated in Fig. 2.

III. LIMITATIONS ON HIDING AND MASKING QUANTUM INFORMATION

A. Stronger no-hiding and no-masking theorems

Let $\mathscr{S} \subseteq \mathscr{D}(\mathcal{H})$ be a set of density matrices. The set $\mathscr{S}$ is IC if $\mathrm{span}(\mathscr{S}) = \mathrm{span}(\mathscr{D}(\mathcal{H}))$. In this case, any other density matrix is uniquely determined by the overlaps (transition probabilities) with density matrices in the set. This definition is motivated by an analogous definition for quantum measurements, usually represented by positive operator-valued measures (POVMs) [37–39]. By virtue of this concept, we can strengthen the no-hiding and no-masking theorems [10,11],
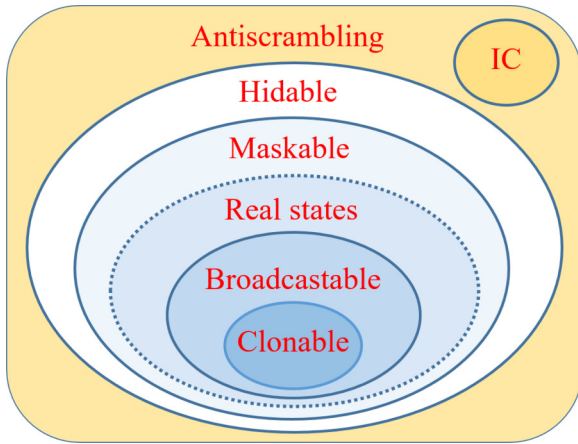
FIG. 2. Hierarchy of no-go theorems and associated sets of quantum states. A set of quantum states can be cloned iff distinct states are orthogonal, while it can be broadcast iff all states commute with each other [12,13,15]. Any set that can be broadcast is equivalent to a subset of the set $\mathscr{D}^R(\mathcal{H})$ of real states, which can be masked even with a real masker. Any maskable set can hide from one party in a nontrivial way. So no-hiding and no-masking theorems do not apply to real quantum mechanics. By contrast, any IC set is antiscrambling (cannot hide from one party in a nontrivial way). Note that the set marked by "Antiscrambling" is the complement of the set marked by "Hidable," as indicated by the color coding.

which is instructive to understanding the distinctions between complex quantum mechanics and real quantum mechanics. Proposition 1 below follows from the very definitions.

Proposition 1. If $\mathrm{span}(\mathscr{S}_1) \subseteq \mathrm{span}(\mathscr{S}_2) \subseteq \mathscr{D}(\mathcal{H})$, then $\mathscr{S}_1$ is maskable whenever $\mathscr{S}_2$ is. If $\mathrm{span}(\mathscr{S}_1) = \mathrm{span}(\mathscr{S}_2)$; then $\mathscr{S}_1$ is hidable or maskable iff $\mathscr{S}_2$ is.

Theorem 1. Any IC set of quantum states is antiscrambling.

Theorem 1 follows from Ref. [10] and proposition 1. It implies theorem 2 below, which also follows from Ref. [11] and proposition 1. Self-contained proofs can be found in Appendix B.

Theorem 2. Any IC set of quantum states is not maskable.

The implications of theorems 1 and 2 are discussed in more detail in the next subsection. Here it should be noted that theorems 1 and 2 do not apply to real quantum mechanics, which is tied to the failure of local tomography [19], as discussed in Appendix B.

B. Implications

To understand the implications of theorems 1 and 2 concerning the limit of hiding and masking quantum information, it is instructive to point out a basic property of IC sets of quantum states. Note that each density matrix on $\mathcal{H}$ can be expressed as $\rho = (\mathbb{1}/d) + \sum_{j=1}^{d^2-1} r_j E_j$, where $\mathbb{1}$ is the identity, $\{E_j\}_{j=1}^{d^2-1}$ is an orthonormal basis in the space of traceless hermitian matrices, and $\boldsymbol{r} = (r_j)_{j=1}^{d^2-1}$ is a generalized Bloch vector. The affine dimension of a set of generalized Bloch vectors is defined as the smallest dimension of affine spaces that contain this set. In this terminology, a set of density matrices is IC iff the (corresponding) set of generalized Bloch

vectors has affine dimension $d^2 - 1$. For a qubit, this fact leads to a simple geometric criterion.

Proposition 2. A set of qubit density matrices is IC iff the set of Bloch vectors is not contained in any disk—the intersection of the Bloch ball with a plane.

In addition, any set of qubit states that is contained in a disk in the Bloch ball is maskable [11,16,17] and thus not antiscrambling. To see this, it suffices to consider pure states. Up to a unitary transformation and irrelevant phase factors, such a set of kets is contained in a set of the form

$$\mathscr{K} = \{\cos\theta |0\rangle + \mathrm{e}^{\mathrm{i}\alpha} \sin\theta |1\rangle \,|\, 0 \leqslant \alpha < 2\pi\}, \qquad (7)$$

where $0 \leqslant \theta \leqslant \pi/4$. This set can be masked by the isometry: $|0\rangle \mapsto |00\rangle, |1\rangle \mapsto |11\rangle$ [11]. So theorems 1 and 2 imply the following corollary.

Corollary 1. A set of qubit states is hidable (or maskable) iff the set is not IC, iff the set of Bloch vectors is contained in a disk.

Corollary 1 confirms the hyperdisk conjecture proposed in Ref. [11] for the qubit case. Here the proof is simpler than previous proofs and has wider applicability [16,17]. This corollary also shows that a nontrivial disk (not a single point) in the qubit case is a maximal maskable set. In particular, $\mathscr{D}^R(\mathcal{H})$ is a maximal maskable set, which is consistent with theorem 4 presented in Sec. V below. Corollary 1 also implies that any hidable or maskable set in the qubit case has measure zero. This conclusion is not a coincidence as confirmed by the following corollary.

Corollary 2. Any hidable set of pure (mixed) states in $\mathscr{P}(\mathcal{H})$ ($\mathscr{D}(\mathcal{H})$) has measure zero with respect to the uniform measure, and so does any maskable set of pure (mixed) states.

Here the uniform measure means the measure induced by the Hilbert-Schmidt distance. In the case of pure states, it coincides with the measure induced by the Haar measure on the unitary group. For pure states, Ref. [26] proved that any maskable set has measure zero given the assumption that the output Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ have the same dimension as $\mathcal{H}$. However, this assumption is too restrictive according to our study on the masking of real quantum states as presented in Sec. V.

Proof. Suppose $\mathscr{S} \in \mathscr{P}(\mathcal{H})$ is hidable. Then $\mathscr{S}$ is not IC according to theorem 1. Therefore we can find a nonzero hermitian operator Q such that $\mathrm{tr}(Q\rho) = 0$ for all $\rho \in \mathscr{S}$, which implies that $\mathscr{S}$ has measure zero within $\mathscr{P}(\mathcal{H})$. A similar proof applies to mixed states and to any hidable or maskable set. ∎

Let t be a positive integer. A weighted set of quantum states $\{|\psi_j\rangle, w_j\}_j$ in $\mathcal{H}$ with $w_j > 0$ is a weighted t-design if $\sum_j w_j(|\psi_j\rangle\langle\psi_j|)^{\otimes t}$ is proportional to the projector onto the symmetric subspace in $\mathcal{H}^{\otimes t}$; it is a t-design if all weights w_j are equal [38,40,41]. Note that any weighted t-design with $t \geqslant 2$ is automatically a weighted 2-design. In addition, the set $\{|\psi_j\rangle\}_j$ is IC if $\{|\psi_j\rangle, w_j\}_j$ is a weighted 2-design for some choice of weights w_j [38,39]. Together with theorems 1 and 2, these observations yield the following corollary.

Corollary 3. Any set of pure states that can form a weighted 2-design is antiscrambling and not maskable.

Prominent examples of 2-designs include symmetric informationally complete (SIC) POVMs [40–42] and complete sets

of $d + 1$ mutually unbiased bases [43–45]. Recall that a SIC POVM in dimension d is composed of d^2 pure states with the equal pairwise fidelity of $1/(d + 1)$. Two bases $\{|\psi_j\rangle\}_j$ and $\{|\phi_k\rangle\}_k$ are mutually unbiased if $|\langle\psi_j|\phi_k\rangle|^2 = 1/d$ for all j, k. A set of mutually unbiased bases in dimension d is complete if it contains $d + 1$ bases. According to Corollary 3, all these sets are antiscrambling and not maskable.

IV. HURWITZ-RADON MATRICES

In this section, we introduce the concept of HR matrices (operators) [27–29], which is crucial to establishing our main result on the masking of real quantum states. Except for lemma 3 below, most results presented in this section are well known [29]. For the convenience of the reader, here we formulate these results in a language that is familiar to researchers in the quantum information community.

A. Definition and basic properties of HR matrices

A set $\{U_j\}_{j=1}^s$ of $m \times m$ unitary matrices (operators) is a set of HR matrices (operators) [27–29] if

$$U_j U_k + U_k U_j = -2\delta_{jk}\mathbb{1}. \tag{8}$$

For example, let $\sigma_x, \sigma_y, \sigma_z$ be the three Pauli matrices; then $\{i\sigma_x, i\sigma_y, i\sigma_z\}$ is a set of HR matrices in dimension 2. Such matrices play crucial roles in the Dirac equation and in the representations of the Clifford algebra [46]. The defining equation above implies that

$$U_j^2 = -\mathbb{1}, \quad U_j^\dagger = -U_j, \quad \mathrm{tr}(U_j^\dagger U_k) = m\delta_{jk}. \tag{9}$$

So each U_j has at most two distinct eigenvalues, namely, i and $-i$; in addition U_j and U_k are orthogonal with respect to the Hilbert-Schmidt inner product when $j \neq k$. If $s \geqslant 2$, then Eq. (8) implies that $\mathrm{tr}(U_j) = 0$ (cf. lemma 3 below); in the case $s = 1$, this conclusion does not hold automatically, and this fact has important implications for the masking of real density matrices, as we shall see later.

The main properties of HR matrices (operators) are summarized below and proved in Appendix C.

Lemma 2. Suppose $U_0, U_1, U_2, \ldots, U_s$ are $s + 1$ unitary matrices of the same size and $\boldsymbol{c} = (c_0, c_1, \ldots, c_s)$ is a real vector of $s + 1$ components; let

$$|\boldsymbol{c}| := \sqrt{\sum_{j=0}^s c_j^2}, \quad U(\boldsymbol{c}) := \sum_{j=0}^s c_j U_j. \tag{10}$$

Then the following statements are equivalent:
(1) $\{U_0^\dagger U_j\}_{j=1}^s$ is a set of s HR matrices.
(2) $U(\boldsymbol{c})^\dagger U(\boldsymbol{c}) = |\boldsymbol{c}|^2\mathbb{1}$ for each real vector $\boldsymbol{c}$.
(3) $U(\boldsymbol{c})$ is unitary for each normalized real vector $\boldsymbol{c}$.

Lemma 3. Suppose $U_0 = \mathbb{1}$ and $\{U_j\}_{j=1}^s$ with $s \geqslant 2$ is a set of HR matrices that commute with a hermitian matrix τ. Suppose j, k, j', k' are integers that satisfy the conditions $0 \leqslant j < k \leqslant s$ and $0 \leqslant j' < k' \leqslant s$; let $\alpha > 0$. Then

$$\mathrm{tr}(U_j U_k \tau^\alpha) = 0, \tag{11}$$

$$\mathrm{tr}(U_j U_k U_{j'} U_{k'} \tau^\alpha) = -\mathrm{tr}(\tau^\alpha)\delta_{jj'}\delta_{kk'}, \quad s \neq 3, \tag{12}$$

$$\mathrm{tr}(U_j U_k U_{j'} U_{k'} \tau^\alpha) = -\mathrm{tr}(\tau^\alpha)\delta_{jj'}\delta_{kk'} + (\delta_{j=0}\epsilon_{kj'k'} + \delta_{j'=0}\epsilon_{jkk'})$$
$$\times \mathrm{tr}(U_1 U_2 U_3 \tau^\alpha), \quad s = 3, \tag{13}$$

where $\epsilon_{kj'k'}$ is equal to 1 (-1) if (k, j', k') is an even (odd) permutation of $(1, 2, 3)$ and is equal to 0 otherwise; $\epsilon_{jkk'}$ is defined in a similar way.

When $\tau = \mathbb{1}$, lemma 3 yields

$$\mathrm{tr}(U_j U_k) = 0, \tag{14}$$

$$\mathrm{tr}(U_j U_k U_{j'} U_{k'}) = -m\delta_{jj'}\delta_{kk'}, \quad s \neq 3, \tag{15}$$

$$\mathrm{tr}(U_j U_k U_{j'} U_{k'}) = -m\delta_{jj'}\delta_{kk'} + (\delta_{j=0}\epsilon_{kj'k'} + \delta_{j'=0}\epsilon_{jkk'})$$
$$\times \mathrm{tr}(U_1 U_2 U_3), \quad s = 3, \tag{16}$$

where $m = \mathrm{tr}(\mathbb{1})$.

B. Construction of HR matrices

In dimension 2, $\{i\sigma_x, i\sigma_y, i\sigma_z\}$ is a set of HR matrices as mentioned before. In higher dimensions, HR matrices can be constructed iteratively. Given a set $\{U_j\}_{j=1}^s$ of s HR matrices in dimension m, then $s + 2$ HR matrices can be constructed in dimension $2m$ as follows,

$$U_j \mapsto U_j \otimes \sigma_z, \quad j = 1, 2, \ldots, s,$$
$$U_{s+1} = \mathbb{1} \otimes i\sigma_x, \quad U_{s+2} = \mathbb{1} \otimes i\sigma_y. \tag{17}$$

In this way, $2b + 1$ HR matrices can be constructed in dimension 2^b, which attain the maximum number according to lemma 4 below. If instead the dimension is divisible by 2^b, then the same number of HR matrices can be constructed by considering the tensor product with a suitable identity matrix.

Suppose $\{U_j\}_{j=1}^r$ and $\{V_j\}_{j=1}^s$ are two sets of HR matrices in dimensions m_1 and m_2, respectively. Then we can construct a set of $r + s + 1$ HR matrices in dimension $2m_1 m_2$ as follows [29]:

$$W_j = \begin{cases} U_j \otimes \mathbb{1} \otimes \sigma_z & 1 \leqslant j \leqslant r, \\ \mathbb{1} \otimes V_{j-r} \otimes \sigma_x & r + 1 \leqslant j \leqslant r + s, \\ \mathbb{1} \otimes \mathbb{1} \otimes i\sigma_y & j = r + s + 1. \end{cases} \tag{18}$$

Note that this construction works even when $r = 0$ and $m_1 = 1$.

HR matrices can also be constructed from real orthogonal matrices. The maximum number of such HR matrices in dimensions 2, 4, 8 are 1, 3, 7, respectively. For example, $i\sigma_y$ is an HR matrix in dimension 2, and $i\sigma_y \otimes \sigma_z, i\sigma_y \otimes \sigma_x, \mathbb{1} \otimes i\sigma_y$ are three HR matrices in dimension 4; seven HR matrices in dimension 8 can be constructed as follows:

$$\sigma_x \otimes i\sigma_y \otimes \mathbb{1}, \quad \sigma_x \otimes \sigma_z \otimes i\sigma_y, \quad \sigma_x \otimes \sigma_x \otimes i\sigma_y,$$
$$i\sigma_y \otimes \mathbb{1} \otimes \mathbb{1}, \quad \sigma_z \otimes \mathbb{1} \otimes i\sigma_y, \quad \sigma_z \otimes i\sigma_y \otimes \sigma_z, \tag{19}$$
$$\sigma_z \otimes i\sigma_y \otimes \sigma_x.$$

Real orthogonal HR matrices in higher dimensions can be constructed iteratively by virtue of Eq. (18), note that W_j is real orthogonal if both U_j and V_{j-r} are real orthogonal. In particular $s + 8$ real orthogonal HR matrices can be constructed in dimension $16m$ if s real orthogonal HR matrices can be constructed in dimension m.

Lemma 4. $d - 1$ unitary (real orthogonal) HR matrices can be constructed in dimension m iff m is divisible by $\kappa(d)$

$(\kappa^R(d))$, where

$$\kappa(d) := 2^{\lfloor (d-1)/2 \rfloor}, \tag{20}$$

$$\kappa^R(d) := \begin{cases} \kappa(d) & d = 0, 1, 7 \quad \mod 8, \\ 2\kappa(d) & d = 2, 3, 4, 5, 6 \quad \mod 8. \end{cases} \tag{21}$$

Lemma 4 follows from Refs. [27–29]. It clarifies the minimum dimension required to construct a given number of HR matrices. Incidentally, the variations of $\kappa(d)$ and $\kappa^R(d)$ exhibit Bott periodicity [29], which is of key interest in algebraic topology.

V. MASKING QUANTUM INFORMATION IN REAL QUANTUM MECHANICS

In this section, we show that the set $\mathscr{D}^R(\mathcal{H})$ of real density matrices is maskable and is actually a maximal maskable set. In addition, we determine the entanglement of masking and the minimum dimension of the output Hilbert space required to mask $\mathscr{D}^R(\mathcal{H})$.

A. Construction of a masker

Let m be an even positive integer that is divisible by $\kappa(d)$. Let $\mathcal{H}_A$ and $\mathcal{H}_B$ be two m-dimensional Hilbert spaces and

$$|\Phi\rangle := \frac{1}{\sqrt{m}} \sum_{l=0}^{m-1} |ll\rangle \tag{22}$$

the canonical maximally entangled state in $\mathcal{H}_A \otimes \mathcal{H}_B$. By assumption we can construct a set $\{U_j\}_{j=1}^{d-1}$ of $d-1$ traceless HR matrices on $\mathcal{H}_A$; let $U_0 = \mathbb{1}_A$. Define the isometry $M : \mathcal{H} \mapsto \mathcal{H}_A \otimes \mathcal{H}_B$ by its action,

$$M|j\rangle = |\Phi_j\rangle := (U_j \otimes \mathbb{1}_B)|\Phi\rangle, \quad j = 0, 1, \ldots, d-1; \tag{23}$$

then M is a masker for $\mathscr{P}^R(\mathcal{H})$ and $\mathscr{D}^R(\mathcal{H})$.

To verify the above claim, note that the d states $|\Phi_j\rangle$ are orthonormal since

$$\langle \Phi_j | \Phi_k \rangle = \frac{1}{m} \mathrm{tr}(U_j^\dagger U_k) = \delta_{jk}. \tag{24}$$

Given any normalized vector $\boldsymbol{c} = (c_0, c_1, \ldots, c_{d-1})$ and the state $|\psi(\boldsymbol{c})\rangle = \sum_j c_j |j\rangle \in \mathcal{H}$, the output state has the form

$$|\Psi(\boldsymbol{c})\rangle = \sum_j c_j |\Phi_j\rangle = [U(\boldsymbol{c}) \otimes \mathbb{1}_B]|\Phi\rangle, \quad U(\boldsymbol{c}) = \sum_j c_j U_j. \tag{25}$$

If in addition $\boldsymbol{c}$ is a real vector, then $U(\boldsymbol{c})$ is unitary by lemma 2 given that $\{U_j\}_{j=1}^{d-1}$ is a set of HR matrices, which implies that $|\Psi(\boldsymbol{c})\rangle$ is maximally entangled. So M is a masker for $\mathscr{P}^R(\mathcal{H})$ and $\mathscr{D}^R(\mathcal{H})$.

If m is divisible by $\kappa^R(d)$ and each U_j is real orthogonal, then the output Hilbert space could be real, which leads to a real masker for $\mathscr{P}^R(\mathcal{H})$ and $\mathscr{D}^R(\mathcal{H})$. Therefore the set of real states can be masked even with a real masker. In other words, the information about quantum states in real quantum mechanics can be completely hidden in the correlations. This fact shows that the no-hiding and no-masking theorems do not apply to real quantum mechanics, in sharp contrast with complex quantum mechanics, as illustrated in Fig. 2.

When $d = 4$ for example, a masker for $\mathscr{D}^R(\mathcal{H})$ can be constructed using the set of HR matrices $\{i\sigma_x, i\sigma_y, i\sigma_z\}$, which is tied to the two-qubit magic basis [30]

$$|\Phi_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad |\Phi_1\rangle = \frac{i}{\sqrt{2}}(|01\rangle + |10\rangle),$$
$$\tag{26}$$
$$|\Phi_2\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle), \quad |\Phi_3\rangle = \frac{i}{\sqrt{2}}(|00\rangle - |11\rangle).$$

Let M be the isometry from $\mathcal{H}$ to the two-qubit Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$ as defined by the map $|j\rangle \mapsto |\Phi_j\rangle$ for $j = 0, 1, 2, 3$. Then M can mask the set $\mathscr{D}^R(\mathcal{H})$. Here the concurrence of the output state $|\Psi(\boldsymbol{c})\rangle = \sum_j c_j |\Phi_j\rangle$ reads [30]

$$C(|\Psi(\boldsymbol{c})\rangle) = \left| \sum_j c_j^2 \right|, \tag{27}$$

so $|\Psi(\boldsymbol{c})\rangle$ is maximally entangled iff $|\psi(\boldsymbol{c})\rangle$ is a real ket up to an overall phase factor. In this way, the masker M establishes a one-to-one correspondence between real pure states in $\mathcal{H}$ and maximally entangled states in $\mathcal{H}_A \otimes \mathcal{H}_B$. This correspondence is tied to the geometric facts that normalized real kets in $\mathcal{H}$ form a 3-sphere, and so does the special unitary group SU(2). Incidentally, based on this example, we can construct a hidable set that is not maskable, as shown in Sec. VI later.

B. All maskers for real quantum states

Next, we determine all maskers for the sets $\mathscr{P}^R(\mathcal{H})$ and $\mathscr{D}^R(\mathcal{H})$. Let $|\Psi_0\rangle$ be any bipartite ket in $\mathcal{H}_A \otimes \mathcal{H}_B$ and $\tau_A = \mathrm{tr}_B(|\Psi_0\rangle\langle\Psi_0|)$. Suppose $\{U_j\}_{j=1}^{d-1}$ is a set of HR matrices that commute with τ_A and satisfy $\mathrm{tr}(U_j\tau_A) = 0$ for $j = 1, 2, \ldots, d-1$ [the condition $\mathrm{tr}(U_j\tau_A) = 0$ is automatically guaranteed when $d \geqslant 3$ thanks to lemma 3]. Let

$$|\Psi_j\rangle = (U_j \otimes \mathbb{1}_B)|\Psi_0\rangle; \tag{28}$$

then the kets $|\Psi_j\rangle$ for $j = 0, 1, \ldots, d-1$ are orthonormal, and the isometry $M : j \mapsto |\Psi_j\rangle$ is a masker for $\mathscr{P}^R(\mathcal{H})$ and $\mathscr{D}^R(\mathcal{H})$. The following theorem proved in Appendix D shows that essentially all maskers can be constructed in this way. It implies corollaries 4-6 below, which are proved in Appendix E.

Theorem 3. Suppose the isometry $M : \mathcal{H} \mapsto \mathcal{H}_A \otimes \mathcal{H}_B$ is a masker for $\mathscr{D}^R(\mathcal{H})$ with common reduced density matrices τ_A and τ_B of full rank. Let $|\Psi_j\rangle := M|j\rangle$. Then $|\Psi_j\rangle$ for $j = 1, 2, \ldots, d-1$ have the form

$$|\Psi_j\rangle = (U_j \otimes \mathbb{1}_B)|\Psi_0\rangle = (\mathbb{1}_A \otimes V_j)|\Psi_0\rangle, \tag{29}$$

where $\{U_j\}_{j=1}^{d-1}$ and $\{V_j\}_{j=1}^{d-1}$ are two sets of HR matrices. Meanwhile, U_j and V_j commute with τ_A and τ_B, respectively, and satisfy $\mathrm{tr}(U_j\tau_A) = \mathrm{tr}(V_j\tau_B) = 0$.

Corollary 4. When $d \geqslant 3$, there exists a complex (real) masker for $\mathscr{D}^R(\mathcal{H})$ with masking spectrum $\{\lambda_o, m_o\}_o$ iff the multiplicity m_o of each nonzero eigenvalue λ_o is divisible by $\kappa(d)$ $(\kappa^R(d))$. When $d = 2$, the same conclusion holds for a real masker; there exists a complex masker for $\mathscr{D}^R(\mathcal{H})$ with masking spectrum $\{\mu_l\}_l$ iff there exists a vector $\boldsymbol{v} = (v_l)_l$ composed of 1 and -1 such that $\sum_l v_l\mu_l = 0$.

Here λ_o refer to distinct eigenvalues, while μ_l for different l may equal each other.

Corollary 5. $\mathscr{D}^{\mathrm{R}}(\mathcal{H})$ can be masked in the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$ iff $d_A, d_B \geqslant \tilde{\kappa}(d) := \max\{\kappa(d), 2\}$; if the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$ is real, then the condition turns into $d_A, d_B \geqslant \kappa^{\mathrm{R}}(d)$.

Given a density matrix $\rho \in \mathscr{D}(\mathcal{H})$, the robustness of imaginarity $\mathscr{I}_{\mathrm{R}}(\rho)$ [24,25] is defined as

$$\mathscr{I}_{\mathrm{R}}(\rho) := \min\left\{ a \geqslant 0 \,\bigg|\, \rho' \in \mathscr{D}(\mathcal{H}), \frac{\rho + a\rho'}{1 + a} \in \mathscr{D}^{\mathrm{R}}(\mathcal{H}) \right\}. \tag{30}$$

A closed formula was presented in Ref. [25], with the result

$$\mathscr{I}_{\mathrm{R}}(\rho) = \tfrac{1}{2}\|\rho - \rho^{\mathrm{T}}\|_1, \tag{31}$$

where $\|\rho - \rho^{\mathrm{T}}\|_1 = \mathrm{tr}\sqrt{(\rho - \rho^{\mathrm{T}})^2}$ is the Schatten 1-norm of $\rho - \rho^{\mathrm{T}}$. Here we are interested in $\mathscr{I}_{\mathrm{R}}(\rho)$ because of its intimate connection with the properties of the output state of any masker for $\mathscr{D}^{\mathrm{R}}(\mathcal{H})$ with $d = \dim(\mathcal{H}) \geqslant 3$ as shown in the following corollary; see also Eq. (46) below. It should be noted that this corollary is not applicable when $d = 2$.

Corollary 6. Suppose $d = \dim(\mathcal{H}) \geqslant 3$ and M is a masker for the set $\mathscr{D}^{\mathrm{R}}(\mathcal{H})$ with common reduced states τ_A and τ_B. Then τ_A (τ_B) is majorized by ϱ_A (ϱ_B) defined in Eq. (1) for all $\rho \in \mathscr{D}^{\mathrm{R}}(\mathcal{H})$. In addition,

$$\mathrm{tr}(\varrho_A^2) + \mathrm{tr}(\varrho_B^2) = \wp(2 + \|\rho - \rho^{\mathrm{T}}\|_{\mathrm{HS}}^2), \tag{32}$$

$$2\wp\left[1 + \frac{2}{d}\mathscr{I}_{\mathrm{R}}(\rho)^2\right] \leqslant \mathrm{tr}(\varrho_A^2) + \mathrm{tr}(\varrho_B^2) \leqslant 2\wp[1 + \mathscr{I}_{\mathrm{R}}(\rho)^2], \tag{33}$$

where $\|\rho - \rho^{\mathrm{T}}\|_{\mathrm{HS}} = \sqrt{\mathrm{tr}[(\rho - \rho^{\mathrm{T}})^2]}$ is the Hilbert-Schmidt norm of $\rho - \rho^{\mathrm{T}}$, and $\wp$ is the masking purity defined in Eq. (5). If in addition $d \neq 4$, then

$$\mathrm{tr}(\varrho_B^2) = \mathrm{tr}(\varrho_A^2) = \tfrac{1}{2}\wp(2 + \|\rho - \rho^{\mathrm{T}}\|_{\mathrm{HS}}^2), \tag{34}$$

$$\wp\left[1 + \frac{2}{d}\mathscr{I}_{\mathrm{R}}(\rho)^2\right] \leqslant \mathrm{tr}(\varrho_A^2) \leqslant \wp[1 + \mathscr{I}_{\mathrm{R}}(\rho)^2]. \tag{35}$$

When $d \geqslant 3$, Eq. (32) implies that

$$\mathrm{tr}(\varrho_A^2) + \mathrm{tr}(\varrho_B^2) \geqslant 2\wp, \tag{36}$$

and the inequality is saturated iff ρ is a real density matrix, that is, $\rho \in \mathscr{D}^{\mathrm{R}}(\mathcal{H})$. If in addition $d \neq 4$, then Eq. (34) implies that

$$\mathrm{tr}(\varrho_A^2) \geqslant \wp, \quad \mathrm{tr}(\varrho_B^2) \geqslant \wp, \tag{37}$$

and each inequality is saturated iff ρ is a real density matrix.

C. Entanglement of masking and masking purity

By virtue of theorem 3 and corollary 4, we can determine the minimum entanglement cost required to mask the set of real quantum states. The following corollary is proved in Appendix F.

Corollary 7. Let E be an entanglement monotone; then

$$E(\mathscr{D}^{\mathrm{R}}(\mathcal{H})) = E(\mathscr{P}^{\mathrm{R}}(\mathcal{H})) = E(|\Phi(\tilde{\kappa}(d))\rangle), \tag{38}$$

$$E^{\mathrm{R}}(\mathscr{D}^{\mathrm{R}}(\mathcal{H})) = E^{\mathrm{R}}(\mathscr{P}^{\mathrm{R}}(\mathcal{H})) = E(|\Phi(\kappa^{\mathrm{R}}(d))\rangle), \tag{39}$$

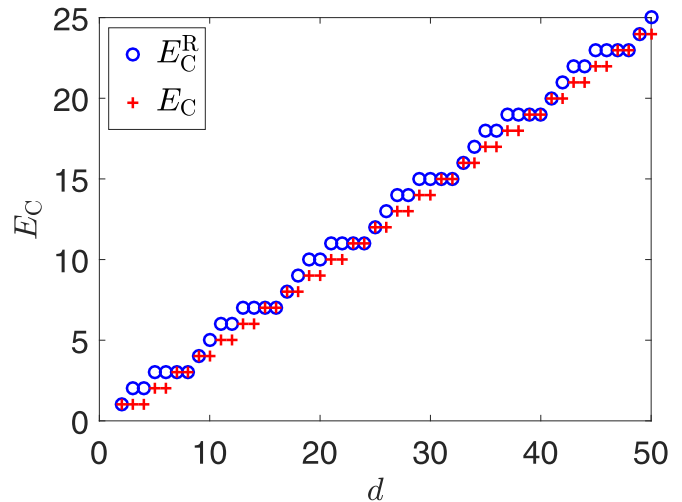where $|\Phi(m)\rangle$ is a maximally entangled state of Schmidt rank m.

FIG. 3. Minimum entanglement cost E_{C} ($E_{\mathrm{C}}^{\mathrm{R}}$) required to mask $\mathscr{P}^{\mathrm{R}}(\mathcal{H})$ and $\mathscr{D}^{\mathrm{R}}(\mathcal{H})$ with complex (real) Hilbert space.

For a bipartite pure state, the entanglement cost, entanglement of formation, distillable entanglement, and relative entropy of entanglement all coincide with the von Neumann entropy of each reduced state [36]. If E is one of these entanglement measures, say, the entanglement cost E_{C}, then corollary 7 and lemma 4 imply that

$$E_{\mathrm{C}}(\mathscr{D}^{\mathrm{R}}(\mathcal{H})) = E_{\mathrm{C}}(\mathscr{P}^{\mathrm{R}}(\mathcal{H})) = \log_2 \tilde{\kappa}(d)$$
$$= \begin{cases} 1 & d = 2, \\ \lfloor \frac{d-1}{2} \rfloor & d \geqslant 3; \end{cases} \tag{40}$$

$$E_{\mathrm{C}}^{\mathrm{R}}(\mathscr{D}^{\mathrm{R}}(\mathcal{H})) = E_{\mathrm{C}}^{\mathrm{R}}(\mathscr{P}^{\mathrm{R}}(\mathcal{H})) = \log_2 \kappa^{\mathrm{R}}(d)$$
$$= \begin{cases} \lfloor \frac{d-1}{2} \rfloor & d = 0, 1, 7 \quad \mathrm{mod}\ 8, \\ \lfloor \frac{d-1}{2} \rfloor + 1 & d = 2, 3, 4, 5, 6 \quad \mathrm{mod}\ 8. \end{cases} \tag{41}$$

Note that $E_{\mathrm{C}}(\mathscr{D}^{\mathrm{R}}(\mathcal{H})) \approx E_{\mathrm{C}}^{\mathrm{R}}(\mathscr{D}^{\mathrm{R}}(\mathcal{H})) \approx d/2$. The entanglement of masking quantified by the entanglement cost E_{C} is approximately linear in d, and the deviation exhibits Bott periodicity, as illustrated in Fig. 3

If the concurrence C [30–32] is chosen to quantify the entanglement, then we have

$$C(\mathscr{D}^{\mathrm{R}}(\mathcal{H})) = C(\mathscr{P}^{\mathrm{R}}(\mathcal{H})) = \sqrt{2[1 - \tilde{\kappa}(d)^{-1}]}, \tag{42}$$

$$C(\mathscr{D}^{\mathrm{R}}(\mathcal{H})) = C(\mathscr{P}^{\mathrm{R}}(\mathcal{H})) = \sqrt{2[1 - \kappa^{\mathrm{R}}(d)^{-1}]}. \tag{43}$$

In addition, corollary 4 implies that the masking purity $\wp$ of any masker for $\mathscr{D}^{\mathrm{R}}(\mathcal{H})$ satisfies $\wp \leqslant 1/\tilde{\kappa}(d)$ (cf. the proof of corollary 7); by contrast, $\wp \leqslant 1/\kappa^{\mathrm{R}}(d)$ for any real masker. This conclusion is expected given the close connection between the concurrence of a bipartite pure state and the purity of each reduced state.

D. Real quantum mechanics as a maximal maskable subtheory

Here we show that the set $\mathscr{D}^{\mathrm{R}}(\mathcal{H})$ of real density matrices is a maximal maskable set within $\mathscr{D}(\mathcal{H})$. Such maximal maskable sets are valuable to understanding the potential and limit of hiding and masking quantum information. However, no maximal maskable sets beyond the qubit system have

been found before the current study as far as we know. This conclusion shows that real quantum mechanics is a maximal maskable subtheory in the usual quantum mechanics. Theorems 4 and 5 below are proved in Appendix G.

Theorem 4. $\mathscr{D}^{\mathrm{R}}(\mathcal{H})$ is a maximal maskable set.

Theorem 4 implies that $\mathscr{P}^{\mathrm{R}}(\mathcal{H})$ is a maximal maskable set within $\mathscr{P}(\mathcal{H})$. Moreover, given any masker M for $\mathscr{D}(\mathcal{H})$ with $d = \dim(\mathcal{H}) \geqslant 3$, it turns out $M(\mathscr{P}^{\mathrm{R}}(\mathcal{H}))$ happens to be the set of maximally entangled states within $M(\mathscr{D}(\mathcal{H}))$, as shown in the following theorem.

Theorem 5. Suppose $d \geqslant 3$ and $M : \mathcal{H} \mapsto \mathcal{H}_A \otimes \mathcal{H}_B$ is a masker for $\mathscr{D}^{\mathrm{R}}(\mathcal{H})$. Let $|\Psi_0\rangle = M|0\rangle$; then any state in $M(\mathscr{D}(\mathcal{H}))$ can be created from $|\Psi_0\rangle\langle\Psi_0|$ by local operations and classical communication (LOCC). In addition, $E(M(\rho)) \leqslant E(|\Psi_0\rangle\langle\Psi_0|)$ for any entanglement monotone E and all $\rho \in \mathscr{D}(\mathcal{H})$. When E is a convex strict monotone, the upper bound is saturated iff $\rho \in \mathscr{P}^{\mathrm{R}}(\mathcal{H})$.

A strict entanglement monotone E means $E(|\Psi_1\rangle) > E(|\Psi_2\rangle)$ whenever $|\Psi_1\rangle$ can be turned into $|\Psi_2\rangle$ by LOCC, but not vice versa. Prominent examples of convex strict monotones include entanglement of formation, entanglement cost, relative entropy of entanglement, and concurrence [30–32,36]. For concurrence, we can further derive the following result (assuming $d \geqslant 3$):

$$C(\varrho) \leqslant \min\left\{\sqrt{2[1 - \mathrm{tr}(\varrho_A^2)]}, \sqrt{2[1 - \mathrm{tr}(\varrho_B^2)]}\right\}$$
$$\leqslant \sqrt{2 - \wp(2 + \|\rho - \rho^{\mathrm{T}}\|_{\mathrm{HS}}^2)} \leqslant \sqrt{2(1 - \wp)}, \quad (44)$$

where $\varrho_A = \mathrm{tr}_B(\varrho)$ and $\varrho_B = \mathrm{tr}_A(\varrho)$ with $\varrho = M(\rho)$. Here the second inequality follows from Eq. (32) in corollary 6. If ρ is pure, then ϱ is pure, and ϱ_A, ϱ_B have the same purity, so the first two inequalities in Eq. (44) are saturated, which yields

$$C(\varrho) = \sqrt{2 - \wp(2 + \|\rho - \rho^{\mathrm{T}}\|_{\mathrm{HS}}^2)} \leqslant \sqrt{2(1 - \wp)} \quad (45)$$

for $d \geqslant 3$. By contrast, the last inequality in Eq. (44) [also in Eq. (45)] is saturated iff ρ is a real density matrix.

For a pure input state ρ, the concurrence $C(M(\rho))$ of the output state is tied to the robustness of imaginarity $\mathscr{I}_{\mathrm{R}}(\rho)$ defined in Eq. (30) [24,25], which plays a key role in the resource theory of imaginarity. In particular, Eqs. (31) and (45) together imply that

$$C(M(\rho)) = \sqrt{2 - 2\wp - 2\wp\mathscr{I}_{\mathrm{R}}^2(\rho)}, \quad d \geqslant 3, \quad (46)$$

note that $\|\rho - \rho^{\mathrm{T}}\|_1 = \sqrt{2}\|\rho - \rho^{\mathrm{T}}\|_{\mathrm{HS}}$ and

$$\mathscr{I}_{\mathrm{R}}(\rho) = \frac{1}{2}\|\rho - \rho^{\mathrm{T}}\|_1 = \frac{1}{\sqrt{2}}\|\rho - \rho^{\mathrm{T}}\|_{\mathrm{HS}} \quad (47)$$

when ρ is pure (which means ρ^{T} is also pure). In this case $C(M(\rho))$ is completely determined by the masking purity $\wp$ and robustness of imaginarity $\mathscr{I}_{\mathrm{R}}(\rho)$. This result is illustrated in Fig. 4 and is of intrinsic interest to the resource theory of imaginarity.

At this point, it should be pointed out that theorem 5 and Eqs. (44)–(46) are not applicable when $d = 2$ since corollary 6 is not applicable in this special case. To construct a
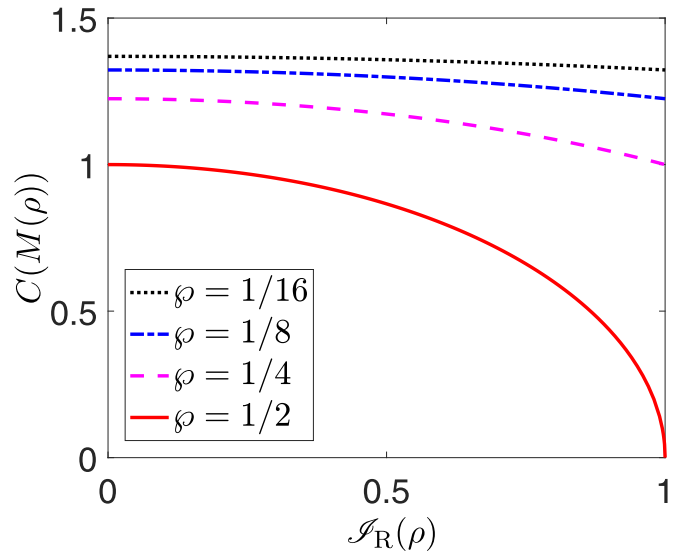

FIG. 4. The relation between the concurrence $C(M(\rho))$ of the output state of the masker M for $\mathscr{D}^{\mathrm{R}}(\mathcal{H})$ and the robustness of imaginarity $\mathscr{I}_{\mathrm{R}}(\rho)$ of the input state. Here ρ is any pure state on $\mathcal{H}$ with $\dim(\mathcal{H}) \geqslant 3$, and $\wp$ is the masking purity of M. The concurrence decreases monotonically with the robustness of imaginarity.

counterexample, let

$$|\Psi_0\rangle = \frac{1}{2}|00\rangle + \frac{1}{2}|11\rangle + \frac{1}{\sqrt{2}}|22\rangle,$$
$$|\Psi_1\rangle = \frac{i}{2}|00\rangle + \frac{i}{2}|11\rangle - \frac{i}{\sqrt{2}}|22\rangle. \quad (48)$$

Then $|\Psi_0\rangle, |\Psi_1\rangle$ are orthonormal, and the isometry M defined by the map $|j\rangle \mapsto |\Psi_j\rangle$ for $j = 0, 1$ is a masker for $\mathscr{D}^{\mathrm{R}}(\mathcal{H})$ with masking purity $\wp = 3/8$ [cf. Eq. (E4) in Appendix E]. Let

$$|\psi\rangle = \frac{1}{6}\left[\sqrt{6(3 - 2\sqrt{2})}|0\rangle - i\sqrt{6(3 + 2\sqrt{2})}|1\rangle\right]; \quad (49)$$

then

$$M|\psi\rangle = \frac{1}{6}\left[\sqrt{6(3 - 2\sqrt{2})}|\Psi_0\rangle - i\sqrt{6(3 + 2\sqrt{2})}|\Psi_1\rangle\right]$$
$$= \frac{1}{\sqrt{3}}(|00\rangle + |11\rangle - |22\rangle). \quad (50)$$

According to the majorization criterion [47], $M|\psi\rangle$ can be turned into $|\Psi_0\rangle$ by LOCC, but not vice versa. Therefore $E(M(|\psi\rangle\langle\psi|)) \geqslant E(|\Psi_0\rangle\langle\Psi_0|)$ for any entanglement monotone E, and the inequality is strict when E is the entanglement cost, entanglement of formation, distillable entanglement, relative entropy of entanglement, or concurrence, which contradicts theorem 5. For example, the concurrence of $M(|\psi\rangle\langle\psi|)$ reads

$$C(M(|\psi\rangle\langle\psi|)) = \frac{2}{\sqrt{3}} > \sqrt{2(1 - \wp)} = \frac{\sqrt{5}}{2}, \quad (51)$$

which contradicts Eqs. (44)–(46).

VI. A HIDABLE SET THAT IS NOT MASKABLE

In this section, we provide an example which is hidable but not maskable. Such an example has never been constructed in the literature previously as far as we know. Suppose $\dim(\mathcal{H}) = 4$ and $\mathscr{S} \subset \mathscr{D}(\mathcal{H})$ is the set of density matrices $\rho = \sum_{j,k=0}^{3} \rho_{jk}|j\rangle\langle k|$ defined by the following constraints

$$\Im\rho_{01} = \Im\rho_{23}, \quad \Im\rho_{02} = -\Im\rho_{13}, \quad \Im\rho_{03} = \Im\rho_{12}, \quad (52)$$

where $\Im$ denotes the imaginary part of a complex number. Then $\mathscr{S}$ contains $\mathscr{D}^{\mathrm{R}}(\mathcal{H})$ as a strict subset and is thus not maskable according to theorem 4. Nevertheless, $\mathscr{S}$ is hidable as we shall see shortly.

To show that $\mathscr{S}$ is hidable, it suffices to construct a nontrivial partial masker for $\mathscr{S}$. Consider the masker M for $\mathscr{D}^{\mathrm{R}}(\mathcal{H})$ that is constructed using the magic basis in Eq. (26). Although M is not a masker for $\mathscr{S}$, it is straightforward to verify that

$$\mathrm{tr}_B[M(\rho)] = \frac{\mathbb{1}_A}{2} \quad \forall \rho \in \mathscr{S}. \quad (53)$$

Therefore M is a partial masker for $\mathscr{S}$. This partial masker is nontrivial because the information about all real quantum states in $\mathscr{S}$ is encoded in the correlations. This example demonstrates that not all hidable sets of quantum states are maskable. In other words, not all sets of quantum states that are not maskable are antiscrambling; the property of being antiscrambling is much stronger, as illustrated in Fig. 2.

VII. RELATION BETWEEN REAL STATES AND PHASE-PARAMETERIZED STATES

Let $\boldsymbol{c} = (c_0, c_1, \ldots, c_{d-1})$ be a normalized real vector with $d \geqslant 2$ and $c_j > 0$ for $j = 0, 1, \ldots, d-1$; define

$$\mathscr{K}(\boldsymbol{c}) = \left\{ \sum_j c_j \mathrm{e}^{\mathrm{i}\phi_j}|j\rangle \,\middle|\, 0 \leqslant \phi_j < 2\pi, j = 0, 1, \ldots, d-1 \right\}. \quad (54)$$

Let $\mathscr{P}(\boldsymbol{c})$ be the set of phase-parameterized states associated with kets in $\mathscr{K}(\boldsymbol{c})$ and let $\overline{\mathscr{P}}(\boldsymbol{c})$ be the convex hull of $\mathscr{P}(\boldsymbol{c})$. According to Ref. [11], the sets $\mathscr{P}(\boldsymbol{c})$ and $\overline{\mathscr{P}}(\boldsymbol{c})$ can be masked by the isometry defined as follows,

$$|j\rangle \mapsto |jj\rangle, \quad j = 0, 1, \ldots d-1. \quad (55)$$

This isometry is well known although it was not recognized as a masker before the study in Ref. [11]. Here the dimension of each subsystem of the output system is the same as that of the input system, which is much smaller compared with the counterpart for masking the set of real quantum states as discussed in Sec. V. Moreover, Ref. [11] conjectured that any maskable set can be embedded in $\overline{\mathscr{P}}(\boldsymbol{c})$ for a suitable choice of $\boldsymbol{c}$, which is known as the hyperdisk conjecture. Although this conjecture has been disproved [17], it is plausible that $\overline{\mathscr{P}}(\boldsymbol{c})$ is a maximal maskable set.

Conjecture 1. Suppose $c_j > 0$ for $j = 0, 1, \ldots, d-1$; then $\overline{\mathscr{P}}(\boldsymbol{c})$ is a maximal maskable set.

Here we clarify the relation between the set $\mathscr{P}(\boldsymbol{c})$ of phase-parameterized states defined above and the set $\mathscr{P}^{\mathrm{R}}(\mathcal{H}')$ of real states. For generality, here $\mathcal{H}'$ is a Hilbert space whose dimension may be different from that of $\mathcal{H}$. When $d = 2$ and $c_0 = c_1 = 1/\sqrt{2}$, the set $\mathscr{P}(\boldsymbol{c})$ corresponds to a great circle on the Bloch sphere and is equivalent to the set $\mathscr{P}^{\mathrm{R}}(\mathcal{H}')$ with $\dim(\mathcal{H}') = 2$. Here "equivalent" means that $\mathscr{P}(\boldsymbol{c})$ can be mapped to $\mathscr{P}^{\mathrm{R}}(\mathcal{H}')$ by some isometry S, that is

$$S\mathscr{P}(\boldsymbol{c})S^{\dagger} = \mathscr{P}^{\mathrm{R}}(\mathcal{H}'). \quad (56)$$

It turns out this is the only case in which $\mathscr{P}(\boldsymbol{c})$ is equivalent to a subset of $\mathscr{P}^{\mathrm{R}}(\mathcal{H}')$, as shown in proposition 3 below and proved in Appendix H. Conversely, $\mathscr{P}^{\mathrm{R}}(\mathcal{H}')$ is equivalent to a subset of $\mathscr{P}(\boldsymbol{c})$ only if $\dim(\mathcal{H}') = 2$, as shown in proposition 4 below and proved in Appendix H.

Proposition 3. Suppose $\mathscr{P}(\boldsymbol{c})$ with $d \geqslant 2$ is equivalent to a subset of $\mathscr{P}^{\mathrm{R}}(\mathcal{H}')$; then $d = 2$ and $c_0 = c_1 = 1/\sqrt{2}$.

Proposition 4. Suppose $\mathscr{P}^{\mathrm{R}}(\mathcal{H}')$ with $\dim(\mathcal{H}') \geqslant 2$ is equivalent to a subset of $\mathscr{P}(\boldsymbol{c})$; then $\dim(\mathcal{H}') = 2$.

Propositions 3 and 4 still hold if $\mathscr{P}(\boldsymbol{c})$ is replaced by $\overline{\mathscr{P}}(\boldsymbol{c})$ and $\mathscr{P}^{\mathrm{R}}(\mathcal{H}')$ is replaced by $\mathscr{D}^{\mathrm{R}}(\mathcal{H}')$. By proposition 4, the set $\mathscr{D}^{\mathrm{R}}(\mathcal{H}')$ with $\dim(\mathcal{H}') \geqslant 3$ cannot be embedded in $\overline{\mathscr{P}}(\boldsymbol{c})$ irrespective of the choice of $\boldsymbol{c}$, which disproves again the hyperdisk conjecture posed in Ref. [11] (cf. Ref. [17]). This conclusion is consistent with the fact that $\mathscr{D}^{\mathrm{R}}(\mathcal{H}')$ is a maximal maskable set as shown in theorem 4. On the other hand, except for the special case specified in proposition 3, $\overline{\mathscr{P}}(\boldsymbol{c})$ cannot be embedded in $\mathscr{D}^{\mathrm{R}}(\mathcal{H}')$, so any maximal maskable set containing $\overline{\mathscr{P}}(\boldsymbol{c})$ cannot be equivalent to $\mathscr{D}^{\mathrm{R}}(\mathcal{H}')$. Quite likely, $\overline{\mathscr{P}}(\boldsymbol{c})$ is itself a maximal maskable set as stated in conjecture 1. In any case, propositions 3 and 4 imply that there exist inequivalent maximal maskable sets, which reflects the complexity of the masking problem.

VIII. SUMMARY

We showed that it is impossible to hide or mask any set of quantum states that is IC, which strengthens the no-hiding and no-masking theorems and establishes an information theoretical underpinning of these no-go results. In sharp contrast, quantum information can be completely hidden in correlations for real quantum mechanics, although the minimum dimension of the output Hilbert space has to increase exponentially with the dimension of the original Hilbert space. Moreover, in a precise sense real quantum mechanics is a maximal maskable subtheory within complex quantum mechanics.

Our study offers valuable insight on the potential and limit of hiding and masking quantum information, which are of intrinsic interest to foundational studies. Meanwhile, the masking protocols we constructed are useful to quantum secret sharing and quantum communication. This is the case in particular when quantum states with real density matrices are easier to prepare and manipulate, say, in linear optics [25]. Furthermore, our study may shed light on a number of other active research areas, including information scrambling and the black-hole information paradox. Notably, the no-hiding theorem derived in Ref. [10] aggravates the tension between unitarity and Hawking's semiclassical analysis of black-hole radiation. The tension would not be so serious in real quantum mechanics thanks to the breakdown of the no-hiding theorem. In addition, our study indicates that Bott periodicity might play an important role in these research areas. We hope that our work can stimulate further progresses in these research topics.

ACKNOWLEDGMENTS

APPENDIX

In this Appendix, we prove the key results presented in the main text, including lemmas 1–3, theorems 1–5, corollaries 4–7, and propositions 3, 4. For the convenience of the readers, lemmas, theorems, corollaries, and propositions will be restated before their proofs. In the course of study, we also derive a few auxiliary results on bipartite pure states and on the masking of real quantum states, which are of some independent interest.

APPENDIX A: PROOF OF LEMMA 1

Lemma 1. Suppose $\mathscr{S}$ contains a pure state ρ_0 and M is a masker for $\mathscr{S}$. Then $E(\mathscr{S}, M) = E(M(\rho_0))$ for any entanglement monotone E.

Proof of lemma 1. Suppose the masker M is an isometry from $\mathcal{H}$ to $\mathcal{H}_A \otimes \mathcal{H}_B$. Let $\varrho_0 = M(\rho_0)$ and $\tau_A = \mathrm{tr}_B(\varrho_0)$. Let ρ be an arbitrary quantum state in $\mathscr{S}$ and $\varrho = M(\rho)$; then $\mathrm{tr}_B(\varrho) = \tau_A$ given that M is a masker for $\mathscr{S}$. Let $|\Psi_\varrho\rangle$ and $|\Psi_{\varrho_0}\rangle$ be purifications of ϱ and ϱ_0, respectively, in $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$, where $\mathcal{H}_C$ is a suitable Hilbert space. Then

$$\mathrm{tr}_C(|\Psi_\varrho\rangle\langle\Psi_\varrho|) = \varrho, \quad \mathrm{tr}_C(|\Psi_{\varrho_0}\rangle\langle\Psi_{\varrho_0}|) = \varrho_0; \quad \text{(A1)}$$

$$\mathrm{tr}_{BC}(|\Psi_\varrho\rangle\langle\Psi_\varrho|) = \mathrm{tr}_{BC}(|\Psi_{\varrho_0}\rangle\langle\Psi_{\varrho_0}|) = \tau_A \quad \forall \varrho \in M(\mathscr{S}). \quad \text{(A2)}$$

The last equation implies that

$$E(\varrho_0) = E(|\Psi_{\varrho_0}\rangle\langle\Psi_{\varrho_0}|) = E(|\Psi_\varrho\rangle\langle\Psi_\varrho|) \geqslant E(\varrho) \quad \text{(A3)}$$

for all $\varrho \in M(\mathscr{S})$, where $E(|\Psi_{\varrho_0}\rangle\langle\Psi_{\varrho_0}|)$ and $E(|\Psi_\varrho\rangle\langle\Psi_\varrho|)$ refer to the bipartite entanglement of $|\Psi_{\varrho_0}\rangle\langle\Psi_{\varrho_0}|$ and $|\Psi_\varrho\rangle\langle\Psi_\varrho|$ with respect to the partition between A and BC. The two equalities in Eq. (A3) follow from the fact that ϱ_0, $|\Psi_{\varrho_0}\rangle\langle\Psi_{\varrho_0}|$, and $|\Psi_\varrho\rangle\langle\Psi_\varrho|$ have the same nonzero Schmidt coefficients, while the inequality follows from the monotonicity of E under partial trace. As an immediate corollary of Eq. (A3), we can deduce that

$$E(\mathscr{S}, M) = \max_{\rho \in \mathscr{S}} E(M(\rho)) = E(\varrho_0) = E(M(\rho_0)), \quad \text{(A4)}$$

which confirms lemma 1. ∎

APPENDIX B: PROOFS OF THEOREMS 1 AND 2

Theorem 1. Any IC set of quantum states is antiscrambling.

Proof of theorem 1. Thanks to proposition 1, it suffices to consider an IC set that is composed of pure states, in which case it is more convenient to work with kets. Let $\mathscr{K} = \{|\psi_h\rangle\}_h \subset \mathcal{H}$ be an arbitrary set of kets that is IC (which means the corresponding set of states is IC), then $|\mathscr{K}| \geqslant d^2$ with $d = \dim(\mathcal{H})$. Without loss of generality, we can assume that d

of the kets in $\mathscr{K}$, say $|\psi_0\rangle, |\psi_1\rangle, \ldots, |\psi_{d-1}\rangle$, are linearly independent, so they form a basis (not necessarily orthogonal) for $\mathcal{H}$, denoted by $\mathcal{B} := \{|\psi_0\rangle, |\psi_1\rangle, \ldots, |\psi_{d-1}\rangle\}$ henceforth. Let $\tilde{\mathcal{B}} = \{|\tilde{\phi}_0\rangle, |\tilde{\phi}_1\rangle, \ldots, |\tilde{\phi}_{d-1}\rangle\}$ be the dual basis of $\mathcal{B}$ defined by the requirement $\langle\tilde{\phi}_j|\psi_k\rangle = \delta_{jk}$, where the tilde is used to indicate that the kets $|\tilde{\phi}_j\rangle$ are not necessarily normalized. Here and in the rest of this proof we assume that j, k can take on the values $0, 1, \ldots, d-1$.

Suppose M is an isometry from $\mathcal{H}$ to $\mathcal{H}_A \otimes \mathcal{H}_B$ and a partial masker for the set $\mathscr{K}$. Let $|\Psi_h\rangle = M|\psi_h\rangle$ and $\tau_A = \mathrm{tr}_B(|\Psi_h\rangle\langle\Psi_h|)$; note that τ_A is independent of h by assumption. Suppose τ_A has the spectral decomposition $\tau_A = \sum \lambda_u |a_u\rangle\langle a_u|$, where λ_u are eigenvalues of τ_A and $|a_u\rangle$ form an orthonormal eigenbasis. Then $|\Psi_h\rangle$ can be expressed as follows,

$$|\Psi_h\rangle = \sum_u \sqrt{\lambda_u}|a_u\rangle\big|b_u^{(h)}\big\rangle, \quad \text{(B1)}$$

where the kets $|b_u^{(h)}\rangle$ for a given h are orthonormal. In addition, $\sum_j |\psi_j\rangle\langle\tilde{\phi}_j|$ is the identity operator on $\mathcal{H}$, so

$$|\psi_h\rangle = \sum_j |\psi_j\rangle\langle\tilde{\phi}_j|\psi_h\rangle = \sum_j \mu_{jh}|\psi_j\rangle, \quad \text{(B2)}$$

where $\mu_{jh} = \langle\tilde{\phi}_j|\psi_h\rangle$ and the two summations run over $j = 0, 1, \ldots, d-1$. Accordingly, $|b_u^{(h)}\rangle = \sum_j \mu_{jh}|b_u^{(j)}\rangle$, and the requirement $\langle b_v^{(h)}|b_u^{(h)}\rangle = \delta_{uv}\langle\psi_h|\psi_h\rangle$ implies that

$$\langle\psi_h|R(v, u)|\psi_h\rangle = 0 \quad \forall h, \quad \text{(B3)}$$

where

$$R(v, u) := \sum_{j,k} R_{kj}(v, u)|\tilde{\phi}_k\rangle\langle\tilde{\phi}_j|, \quad \text{(B4)}$$

$$R_{kj}(v, u) := \big\langle b_v^{(k)}\big|b_u^{(j)}\big\rangle - \delta_{uv}\langle\psi_k|\psi_j\rangle. \quad \text{(B5)}$$

By assumption the set $\mathscr{K}$ is IC, so Eq. (B3) implies that $R(v, u) = 0$ and $R_{kj}(v, u) = 0$, that is,

$$\big\langle b_v^{(k)}\big|b_u^{(j)}\big\rangle = \delta_{uv}\langle\psi_k|\psi_j\rangle, \quad j, k = 0, 1, \ldots, d-1. \quad \text{(B6)}$$

Define $|\bar{b}_u^{(j)}\rangle := |u\rangle \otimes |\psi_j\rangle$, where $|u\rangle$ are orthonormal kets in a suitable Hilbert space; then $\langle b_v^{(k)}|b_u^{(j)}\rangle = \langle\bar{b}_v^{(k)}|\bar{b}_u^{(j)}\rangle$. So there exists an isometry that maps $|b_u^{(j)}\rangle$ to $|u\rangle \otimes |\psi_j\rangle$. This isometry induces the following transformation,

$$|\Psi_h\rangle \mapsto \sum_u \sqrt{\lambda_u}|a_u\rangle \otimes (|u\rangle \otimes |\psi_h\rangle), \quad \text{(B7)}$$

which implies that $M|\psi_h\rangle\langle\psi_h|M^\dagger$ have the form in Eq. (3). It follows that the set $\mathscr{K}$ is antiscrambling, which confirms theorem 1. ∎

Theorem 2. Any IC set of quantum states is not maskable.

Proof of theorem 2. Let $\mathscr{K} = \{|\psi_h\rangle\}_h$ be a set of kets in $\mathcal{H}$ that is IC; then $|\mathscr{K}| \geqslant d^2$, where $d = \dim(\mathcal{H})$. Choose d kets in $\mathscr{K}$, say $|\psi_0\rangle, |\psi_1\rangle, \ldots, |\psi_{d-1}\rangle$, that are linearly independent, so they form a basis of $\mathcal{H}$, denoted by $\mathcal{B} := \{|\psi_0\rangle, |\psi_1\rangle, \ldots, |\psi_{d-1}\rangle\}$ henceforth. As in the proof of theorem 1, let $\tilde{\mathcal{B}} = \{|\tilde{\phi}_0\rangle, |\tilde{\phi}_1\rangle, \ldots, |\tilde{\phi}_{d-1}\rangle\}$ be the dual basis of $\mathcal{B}$.

Suppose on the contrary that $\mathscr{K}$ can be masked by the masker M, which maps $\mathcal{H}$ to a subspace of $\mathcal{H}_A \otimes \mathcal{H}_B$.

Let $|\Psi_h\rangle = M|\psi_h\rangle$ for all h; then the two reduced density operators $\tau_A := \mathrm{tr}_B(|\Psi_h\rangle\langle\Psi_h|)$ and $\tau_B := \mathrm{tr}_A(|\Psi_h\rangle\langle\Psi_h|)$ are independent of h by assumption. Suppose τ_A has spectral decomposition $\tau_A = \sum_u \lambda_u |a_u\rangle\langle a_u|$, where the eigenkets $|a_u\rangle$ are orthonormal. Then $|\Psi_h\rangle$ can be expressed as

$$|\Psi_h\rangle = \sum_u \sqrt{\lambda_u} |a_u\rangle |b_u^{(h)}\rangle, \tag{B8}$$

where the kets $|b_u^{(h)}\rangle$ for a given h are orthonormal. Accordingly we have

$$\mathrm{tr}_A(|\Psi_h\rangle\langle\Psi_h|) = \sum_u \lambda_u |b_u^{(h)}\rangle\langle b_u^{(h)}| = \tau_B \quad \forall h. \tag{B9}$$

In addition, each ket $|\psi_h\rangle$ in $\mathscr{K}$ can be expressed as

$$|\psi_h\rangle = \sum_j |\psi_j\rangle\langle\tilde{\phi}_j|\psi_h\rangle = \sum_j \mu_{jh}|\psi_j\rangle, \tag{B10}$$

where $\mu_{jh} = \langle\tilde{\phi}_j|\psi_h\rangle$, so that

$$|\Psi_h\rangle = \sum_j \mu_{jh}|\Psi_j\rangle = \sum_{u,j} \mu_{jh}\sqrt{\lambda_u}|a_u\rangle|b_u^{(j)}\rangle. \tag{B11}$$

Now the requirement $\mathrm{tr}_A(|\Psi_h\rangle\langle\Psi_h|) = \langle\psi_h|\psi_h\rangle\tau_B$ implies that

$$\mathrm{tr}_{\mathcal{H}}[(|\psi_h\rangle\langle\psi_h| \otimes \mathbb{1}_B)\tilde{R}] = 0 \quad \forall h, \tag{B12}$$

where $\mathbb{1}_B$ is the identity operator on $\mathcal{H}_B$ and

$$\tilde{R} := \sum_{j,k} |\tilde{\phi}_k\rangle\langle\tilde{\phi}_j| \otimes \tilde{R}^{(jk)}, \tag{B13}$$

$$\tilde{R}^{(jk)} := \sum_u \lambda_u |b_u^{(j)}\rangle\langle b_u^{(k)}| - \langle\psi_k|\psi_j\rangle\tau_B. \tag{B14}$$

Note that $\tilde{R}$ is a hermitian operator acting on $\mathcal{H} \otimes \mathcal{H}_B$.

By assumption the set $\mathscr{K}$ is IC, so Eq. (B12) implies that $\tilde{R} = 0$, which in turn implies that $\tilde{R}^{(jk)} = 0$ for $j, k = 0, 1, \ldots, d-1$. In conjunction with Eqs. (B9) and (B14), we can deduce the following equality,

$$0 = \langle b_u^{(j)}|\tilde{R}^{(jk)}|b_u^{(k)}\rangle = \lambda_u - \lambda_u\langle\psi_k|\psi_j\rangle\langle b_u^{(j)}|b_u^{(k)}\rangle \;\; \forall u. \tag{B15}$$

However, this equation cannot hold whenever $\lambda_u > 0$ given that $|\langle\psi_k|\psi_j\rangle| < 1$ and $|\langle b_u^{(j)}|b_u^{(k)}\rangle| \leqslant 1$. This contradiction completes the proof of theorem 2. ∎

Here it is instructive to clarify why the above proof does not apply to real quantum mechanics. It is well known that local tomography fails in real quantum mechanics, which means it is in general impossible to determine the state of a composite system by local measurements only [19]. In the case of two qubits, for example, each real density matrix can be expressed as

$$\rho = \tfrac{1}{4}[\mathbb{1} + (a_x\sigma_x + a_z\sigma_z) \otimes \mathbb{1}_B + \mathbb{1}_A \otimes (b_x\sigma_x + b_z\sigma_z)$$
$$+ T_{xx}\sigma_x \otimes \sigma_x + T_{xz}\sigma_x \otimes \sigma_z + T_{zx}\sigma_z \otimes \sigma_x$$
$$+ T_{zz}\sigma_z \otimes \sigma_z + T_{yy}\sigma_y \otimes \sigma_y], \tag{B16}$$

where $\sigma_x, \sigma_y, \sigma_z$ are the three Pauli matrices,

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{B17}$$

and $a_x, a_z, b_x, b_z, T_{xx}, T_{xz}, T_{zx}, T_{zz}, T_{yy}$ are real coefficients. With local measurements only, it is impossible to determine the state ρ completely because such measurements provide no information about the coefficient T_{yy}.

Now, let us turn back to the proof of theorem 2. In real quantum mechanics, due to the failure of local tomography, Eq. (B12) alone does not imply the equality $\tilde{R} = 0$, so the reasoning in the proof of theorem 2 breaks down. Nevertheless, this fact offers little clue on how to construct a masker for the set of real density matrices, so itself does not disprove the no-masking and no-hiding theorems on real quantum mechanics. The maskers we construct in the main text are crucial to settling this issue completely.

APPENDIX C: PROOFS OF LEMMAS 2 AND 3

Lemma 2. Suppose $U_0, U_1, U_2, \ldots, U_s$ are $s+1$ unitary matrices of the same size and $\boldsymbol{c} = (c_0, c_1, \ldots, c_s)$ is a real vector of $s+1$ components; let

$$|\boldsymbol{c}| := \sqrt{\sum_{j=0}^s c_j^2}, \quad U(\boldsymbol{c}) := \sum_{j=0}^s c_j U_j. \tag{10}$$

Then the following statements are equivalent:

(1) $\{U_0^\dagger U_j\}_{j=1}^s$ is a set of s HR matrices.
(2) $U(\boldsymbol{c})^\dagger U(\boldsymbol{c}) = |\boldsymbol{c}|^2 \mathbb{1}$ for each real vector $\boldsymbol{c}$.
(3) $U(\boldsymbol{c})$ is unitary for each normalized real vector $\boldsymbol{c}$.

Proof of lemma 2. Let

$$V_j := U_0^\dagger U_j, \quad V(\boldsymbol{c}) := \sum_{j=0}^s c_j V_j; \tag{C1}$$

then $V_0 = \mathbb{1}$ and $V(\boldsymbol{c}) = U_0^\dagger U(\boldsymbol{c})$. Suppose statement 1 holds, which means $\{V_j\}_{j=1}^s$ is a set of s HR matrices. Then

$$V_j^\dagger = -V_j, \quad V_j V_k + V_k V_j = -2\delta_{jk}\mathbb{1} \quad \forall j, k = 1, 2, \ldots, s. \tag{C2}$$

Therefore

$$V(\boldsymbol{c})^\dagger V(\boldsymbol{c}) = \sum_{j,k} c_j c_k V_j^\dagger V_k$$
$$= |\boldsymbol{c}|^2 \mathbb{1} + \sum_{j<k} c_j c_k (V_j^\dagger V_k + V_k^\dagger V_j) = |\boldsymbol{c}|^2 \mathbb{1}, \tag{C3}$$

which implies that $U(\boldsymbol{c})^\dagger U(\boldsymbol{c}) = |\boldsymbol{c}|^2 \mathbb{1}$ and confirms the implication $1 \Rightarrow 2$. The implication $2 \Rightarrow 3$ is obvious.

Next, suppose statement 3 holds, then the matrix $V(\boldsymbol{c})$ is unitary for each normalized real vector $\boldsymbol{c}$. In particular $(\mathbb{1} + V_j)/\sqrt{2}$ is unitary for $j = 1, 2, \ldots, s$, which implies that $V_j^\dagger = -V_j$ and $V_j^2 = -\mathbb{1}$. In addition, the requirement that $(V_j + V_k)/\sqrt{2}$ is unitary for $1 \leqslant j < k \leqslant s$ implies that

$$0 = V_j^\dagger V_k + V_k^\dagger V_j = -V_j V_k - V_k V_j. \tag{C4}$$

Therefore $\{V_j\}_{j=1}^s$ is a set of s HR matrices, which confirms the implication $3 \Rightarrow 1$. ∎

Lemma 3. Suppose $U_0 = \mathbb{1}$ and $\{U_j\}_{j=1}^s$ with $s \geqslant 2$ is a set of HR matrices that commute with a hermitian matrix τ. Suppose j, k, j', k' are integers that satisfy the conditions

$0 \leqslant j < k \leqslant s$ and $0 \leqslant j' < k' \leqslant s$; let $\alpha > 0$. Then

$$\mathrm{tr}(U_j U_k \tau^\alpha) = 0, \qquad (11)$$

$$\mathrm{tr}(U_j U_k U_{j'} U_{k'} \tau^\alpha) = -\mathrm{tr}(\tau^\alpha)\delta_{jj'}\delta_{kk'}, \quad s \neq 3, \qquad (12)$$

$$\mathrm{tr}(U_j U_k U_{j'} U_{k'} \tau^\alpha) = -\mathrm{tr}(\tau^\alpha)\delta_{jj'}\delta_{kk'} + (\delta_{j=0}\epsilon_{kj'k'} + \delta_{j'=0}\epsilon_{jkk'})$$
$$\times \mathrm{tr}(U_1 U_2 U_3 \tau^\alpha), \quad s = 3, \qquad (13)$$

where $\epsilon_{kj'k'}$ is equal to 1 (-1) if (k, j', k') is an even (odd) permutation of $(1, 2, 3)$ and is equal to 0 otherwise; $\epsilon_{jkk'}$ is defined in a similar way.

Proof of lemma 3. Since $\{U_j\}_{j=1}^s$ is a set of HR matrices, we have

$$U_j U_k + U_k U_j = -2\delta_{jk}\mathbb{1} \quad \forall 1 \leqslant j < k \leqslant s. \qquad (C5)$$

By the assumptions $s \geqslant 2$ and $0 \leqslant j < k \leqslant s$, we can always find a matrix V in $\mathscr{U} := \{U_j\}_{j=1}^s$ that anticommutes with $U_j U_k$. Therefore

$$\mathrm{tr}(U_j U_k \tau^\alpha) = \mathrm{tr}(V U_j U_k \tau^\alpha V^\dagger) = \mathrm{tr}(V U_j U_k V^\dagger \tau^\alpha)$$
$$= -\mathrm{tr}(U_j U_k \tau^\alpha), \qquad (C6)$$

which implies Eq. (11).

Next, we can prove Eq. (12) in the case $s \neq 3$. When $j = j'$ and $k = k'$, Eq. (12) follows from the fact that $(U_j U_k)^2 = -\mathbb{1}$. When $j \neq j'$ or $k \neq k'$, we can always find a matrix $V \in \mathscr{U}$ that anticommutes with $U_j U_k U_{j'} U_{k'}$, which implies that $\mathrm{tr}(U_j U_k U_{j'} U_{k'} \tau^\alpha) = 0$ and confirms Eq. (12).

It remains to prove Eq. (13) in the case $s = 3$. When $j = j'$ and $k = k'$, Eq. (13) follows from the fact that $(U_j U_k)^2 = -\mathbb{1}$ as Eq. (12). When $j = 0$ and (k, j', k') is a permutation of $(1, 2, 3)$, Eq. (13) follows from the fact that $U_k, U_{j'}, U_{k'}$ anticommute with each other. When $j' = 0$ and (j, k, k') is a permutation of $(1, 2, 3)$, Eq. (13) follows from a similar reasoning. In all other cases, we can always find a matrix $V \in \mathscr{U}$ that anticommutes with $U_j U_k U_{j'} U_{k'}$, which implies that $\mathrm{tr}(U_j U_k U_{j'} U_{k'} \tau^\alpha) = 0$ and confirms Eq. (13). ∎

APPENDIX D: PROOF OF THEOREM 3

1. Main proof

Theorem 3. Suppose the isometry $M : \mathcal{H} \mapsto \mathcal{H}_A \otimes \mathcal{H}_B$ is a masker for $\mathscr{D}^{\mathrm{R}}(\mathcal{H})$ with common reduced density matrices τ_A and τ_B of full rank. Let $|\Psi_j\rangle := M|j\rangle$. Then $|\Psi_j\rangle$ for $j = 1, 2, \ldots, d-1$ have the form

$$|\Psi_j\rangle = (U_j \otimes \mathbb{1}_B)|\Psi_0\rangle = (\mathbb{1}_A \otimes V_j)|\Psi_0\rangle, \qquad (29)$$

where $\{U_j\}_{j=1}^{d-1}$ and $\{V_j\}_{j=1}^{d-1}$ are two sets of HR matrices. Meanwhile, U_j and V_j commute with τ_A and τ_B, respectively, and satisfy $\mathrm{tr}(U_j \tau_A) = \mathrm{tr}(V_j \tau_B) = 0$.

Before proving theorem 3, it is worth pointing out that it does not cause any loss of generality to assume that τ_A and τ_B have full rank. Note that all states $|\Psi_j\rangle$ for $j = 0, 1, \ldots, d-1$ have the same reduced density matrix for each party since M is a masker for $\mathscr{D}^{\mathrm{R}}(\mathcal{H})$. In addition, $\mathrm{tr}_B[M(\rho)]$ for each $\rho \in \mathscr{D}(\mathcal{H})$ is supported in the support of τ_A. So we can always replace $\mathcal{H}_A$ with the support of τ_A if necessary. Similarly, we can replace $\mathcal{H}_B$ with the support of τ_B if necessary.

Proof of theorem 3. By assumption each $|\Psi_j\rangle$ for $j = 1, 2, \ldots, d-1$ has the same reduced states as $|\Psi_0\rangle$, so there

exists a unique unitary matrix U_j acting on $\mathcal{H}_A$ and a unique unitary matrix V_j acting on $\mathcal{H}_B$ that satisfy Eq. (29) in theorem 3 according to lemma 5 below. In addition, U_j and V_j commute with τ_A and τ_B, respectively. Furthermore, we have

$$\mathrm{tr}(V_j \tau_B) = \mathrm{tr}(U_j \tau_A) = \langle\Psi_0|\Psi_j\rangle = \langle 0|j\rangle = \delta_{j0} = 0 \quad (D1)$$

since M is an isometry.

Let $\boldsymbol{c} := (c_0, c_1, \ldots, c_{d-1})$ be an arbitrary normalized real vector; let $|\psi(\boldsymbol{c})\rangle = \sum_j c_j|j\rangle$ and $|\Psi(\boldsymbol{c})\rangle = M|\psi(\boldsymbol{c})\rangle$. Then

$$|\Psi(\boldsymbol{c})\rangle = [U(\boldsymbol{c}) \otimes \mathbb{1}_B]|\Psi_0\rangle, \quad U(\boldsymbol{c}) = \sum_{j=0}^{d-1} c_j U_j, \quad (D2)$$

where $U_0 = \mathbb{1}_A$. By assumption $|\Psi(\boldsymbol{c})\rangle$ has the same reduced states as $|\Psi_0\rangle$, so $U(\boldsymbol{c})$ is a unitary matrix that commutes with τ_A according to lemma 5 below. Furthermore, $\{U_j\}_{j=1}^{d-1}$ is a set of $d-1$ HR matrices by lemma 2. Following a similar reasoning, $\{V_j\}_{j=1}^{d-1}$ is a set of $d-1$ HR matrices. ∎

2. An auxiliary lemma

Lemma 5. Suppose $|\Psi_1\rangle, |\Psi_2\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ are bipartite pure states that have the same reduced states τ_A and τ_B for the two parties, respectively, that is,

$$\mathrm{tr}_B(|\Psi_1\rangle\langle\Psi_1|) = \mathrm{tr}_B(|\Psi_2\rangle\langle\Psi_2|) = \tau_A, \qquad (D3)$$

$$\mathrm{tr}_A(|\Psi_1\rangle\langle\Psi_1|) = \mathrm{tr}_A(|\Psi_2\rangle\langle\Psi_2|) = \tau_B, \qquad (D4)$$

where τ_A has full rank on $\mathcal{H}_A$. Then there exists a unique linear operator U acting on $\mathcal{H}_A$ that satisfies

$$|\Psi_2\rangle = (U \otimes \mathbb{1}_B)|\Psi_1\rangle; \qquad (D5)$$

in addition, the operator U is unitary and commutes with τ_A.

The last conclusion in lemma 5 means U is block diagonal with respect to the eigenspaces of τ_A.

Proof. By assumption both $|\Psi_1\rangle$ and $|\Psi_2\rangle$ are purifications of τ_B, so they can be turned into each other by local unitary transformations on $\mathcal{H}_A$. In other words, we can find a unitary operator U acting on $\mathcal{H}_A$ that satisfies Eq. (D5).

Let

$$|\Psi_1\rangle = \sum_{jk} \Psi_{jk}^{(1)}|jk\rangle, \quad |\Psi_2\rangle = \sum_{jk} \Psi_{jk}^{(2)}|jk\rangle \qquad (D6)$$

be the decomposition of $|\Psi_1\rangle$ and $|\Psi_2\rangle$ in the computational basis and define

$$M_1 = \sum_{jk} \Psi_{jk}^{(1)}|j\rangle\langle k|, \quad M_2 = \sum_{jk} \Psi_{jk}^{(2)}|j\rangle\langle k|. \qquad (D7)$$

Then we have

$$M_1 M_1^\dagger = M_2 M_2^\dagger = \tau_A, \quad M_2 = UM_1, \qquad (D8)$$

which imply that

$$M_1 M_1^\dagger \tau_A^{-1} = \mathbb{1}_A, \quad U = M_2 M_1^\dagger \tau_A^{-1}, \qquad (D9)$$

given that τ_A has full rank. So there exists only one linear operator U that can satisfy Eq. (D5).

In addition, Eq. (D8) implies that

$$U\tau_A U^\dagger = \tau_A, \tag{D10}$$

so the unitary operator U commutes with τ_A. ∎

APPENDIX E: PROOFS OF COROLLARIES 4-6

1. Main proofs

Corollary 4. When $d \geqslant 3$, there exists a complex (real) masker for $\mathscr{D}^R(\mathcal{H})$ with masking spectrum $\{\lambda_o, m_o\}_o$ iff the multiplicity m_o of each nonzero eigenvalue λ_o is divisible by $\kappa(d)$ ($\kappa^R(d)$). When $d = 2$, the same conclusion holds for a real masker; there exists a complex masker for $\mathscr{D}^R(\mathcal{H})$ with masking spectrum $\{\mu_l\}_l$ iff there exists a vector $\boldsymbol{v} = (v_l)_l$ composed of 1 and -1 such that $\sum_l v_l \mu_l = 0$.

Proof of corollary 4. Suppose $d \geqslant 3$ and each m_o is divisible by $\kappa(d)$. Let $m = \sum_o m_o$ and let $\mathcal{H}_A$ and $\mathcal{H}_B$ be two m-dimensional Hilbert spaces, which are isomorphic. Let $|\Psi_0\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ be any ket whose reduced state τ_A for party A has spectrum $\{\lambda_o, m_o\}_o$. Let $\mathcal{H}_o$ be the eigenspace of τ_A associated with λ_o, then $\mathcal{H}_o$ has dimension m_o. By lemma 4, we can construct a set $\{V_{o,j}\}_{j=1}^{d-1}$ of $d-1$ HR matrices for each subspace $\mathcal{H}_o$. Let $U_j = \bigoplus_o V_{o,j}$ for $j = 1, 2, \ldots, d-1$; then $\{U_j\}_{j=1}^{d-1}$ is a set of HR matrices that commute with τ_A.

Define

$$|\Psi_j\rangle = (U_j \otimes \mathbb{1}_B)|\Psi_0\rangle, \quad j = 1, 2, \ldots, d-1 \tag{E1}$$

as in the main text. Then

$$\langle\Psi_0|\Psi_j\rangle = \mathrm{tr}(U_j \tau_A) = 0 \quad \forall j = 1, 2, \ldots, d-1, \tag{E2}$$

$$\langle\Psi_k|\Psi_j\rangle = \mathrm{tr}(U_k^\dagger U_j \tau_A) = \delta_{jk} \quad \forall j, k = 1, 2, \ldots, d-1, \tag{E3}$$

given that U_k anticommutes with U_j and $U_k^\dagger U_j$ for $j \neq k$ (cf. lemma 3), so the d kets $|\Psi_j\rangle$ for $j = 0, 1, \ldots, d-1$ are orthonormal. In addition, $\sum_j c_j U_j$ is unitary for any normalized real vector $\boldsymbol{c} = (c_j)_j$. So the isometry M determined by the map $|j\rangle \mapsto |\Psi_j\rangle$ for $j = 0, 1, \ldots, d-1$ is a masker for $\mathscr{P}^R(\mathcal{H})$ and $\mathscr{D}^R(\mathcal{H})$ with masking spectrum $\{\lambda_o, m_o\}_o$.

Conversely, if there exists a masker with masking spectrum $\{\lambda_o, m_o\}_o$, then theorem 3 implies that there exists a set of

$d-1$ HR matrices in dimension m_o for each o. Therefore m_o is divisible by $\kappa(d)$ according to lemma 4.

When $d \geqslant 2$ and m_o is divisible by $\kappa^R(d)$, a real masker can be constructed as long as $|\Psi_0\rangle$ is a real ket and $\{V_{o,j}\}_{j=1}^{d-1}$ for each o is a set of real orthogonal HR matrices. In this case, τ_A is symmetric, while each U_j is antisymmetric, so Eqs. (E2) and (E3) hold even when $d = 2$.

Conversely, the existence of a real masker with masking spectrum $\{\lambda_o, m_o\}_o$ implies that each m_o is divisible by $\kappa^R(d)$ according to a similar reasoning employed above.

It remains to consider complex maskers for a qubit (with $d = 2$). Suppose there exists a real vector $v = (v_l)_l$ composed of 1 and -1 that satisfies the equality $\sum_l v_l \mu_l = 0$. Let $U = \sum_l \mathrm{i} v_l |l\rangle\langle l|$ and

$$|\Psi_0\rangle = \sum_l \sqrt{\mu_l}|ll\rangle,$$
$$|\Psi_1\rangle = (U \otimes \mathbb{1}_B)|\Psi_0\rangle = \mathrm{i}\sum_l v_l \sqrt{\mu_l}|ll\rangle. \tag{E4}$$

Then $|\Psi_0\rangle, |\Psi_1\rangle$ are orthonormal, and the isometry M defined by the map $|j\rangle \mapsto |\Psi_j\rangle$ for $j = 0, 1$ is a masker for $\mathscr{D}^R(\mathcal{H})$.

Conversely, suppose M is a masker for the set $\mathscr{D}^R(\mathcal{H})$ with masking spectrum $\{\mu_l\}_l$. Let $|\Psi_0\rangle = M|0\rangle$ and $\tau_A = \mathrm{tr}_B(|\Psi_0\rangle\langle\Psi_0|)$. Without loss of generality, we can assume that τ_A has full rank. According to theorem 3, there exists an HR matrix U that commutes with τ_A and satisfies $\mathrm{tr}(U\tau_A) = 0$. By a suitable choice of orthonormal basis if necessary, we can assume that both U and τ_A are diagonal. The diagonal entries of τ_A happen to be μ_l, while the diagonal entries of U have the form $v_l \mathrm{i}$ with $v_l = \pm 1$, given that each eigenvalue of U is either i or $-\mathrm{i}$. Therefore $\mathrm{i}\sum_l v_l \mu_l = \mathrm{tr}(U\tau_A) = 0$, which completes the proof of corollary 4. ∎

Corollary 5. $\mathscr{D}^R(\mathcal{H})$ can be masked in the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$ iff $d_A, d_B \geqslant \tilde{\kappa}(d) := \max\{\kappa(d), 2\}$; if the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$ is real, then the condition turns into $d_A, d_B \geqslant \kappa^R(d)$.

Proof of corollary 5. Corollary 5 is an immediate consequence of corollary 4. ∎

Corollary 6. Suppose $d = \dim(\mathcal{H}) \geqslant 3$ and M is a masker for the set $\mathscr{D}^R(\mathcal{H})$ with common reduced states τ_A and τ_B. Then τ_A (τ_B) is majorized by ϱ_A (ϱ_B) defined in Eq. (1) for all $\rho \in \mathscr{D}(\mathcal{H})$. In addition,

$$\mathrm{tr}(\varrho_A^2) + \mathrm{tr}(\varrho_B^2) = \wp(2 + \|\rho - \rho^T\|_{HS}^2), \tag{32}$$

$$2\wp\left[1 + \frac{2}{d}\mathscr{I}_R(\rho)^2\right] \leqslant \mathrm{tr}(\varrho_A^2) + \mathrm{tr}(\varrho_B^2) \leqslant 2\wp[1 + \mathscr{I}_R(\rho)^2], \tag{33}$$

where $\|\rho - \rho^T\|_{HS} = \sqrt{\mathrm{tr}[(\rho - \rho^T)^2]}$ is the Hilbert-Schmidt norm of $\rho - \rho^T$, and $\wp$ is the masking purity defined in Eq. (5). If in addition $d \neq 4$, then

$$\mathrm{tr}(\varrho_B^2) = \mathrm{tr}(\varrho_A^2) = \tfrac{1}{2}\wp(2 + \|\rho - \rho^T\|_{HS}^2), \tag{34}$$

$$\wp\left[1 + \frac{2}{d}\mathscr{I}_R(\rho)^2\right] \leqslant \mathrm{tr}(\varrho_A^2) \leqslant \wp[1 + \mathscr{I}_R(\rho)^2]. \tag{35}$$

Proof of corollary 6. Without loss of generality, we can assume that τ_A and τ_B have full rank. Let $|\Psi_j\rangle = M|j\rangle$, then $|\Psi_j\rangle$ have the form in Eq. (29) according to theorem 3, so ϱ_A and ϱ_B have the form in Eqs. (E15) and (E16) according to lemma 6 below. In addition, ϱ_A and ϱ_B commute with τ_A and τ_B, respectively. Let P be the projector onto the eigenspace of τ_A associated with

any nonzero eigenvalue λ; then P commutes with ϱ_A. Meanwhile, $\mathrm{tr}(PU_jU_k) = 0$ for $0 \leqslant j < k < d$ since we can always find a matrix in $\{U_j\}_{j=1}^{d-1}$ that anticommutes with U_jU_k (note that this conclusion does not hold when $d = 2$, and that is why we assume $d \geqslant 3$ in corollary 6). Therefore

$$\mathrm{tr}(P\varrho_A) = \mathrm{tr}(P\tau_A) + \sum_{0 \leqslant j < k < d} (\rho_{kj} - \rho_{jk})\,\mathrm{tr}(PU_jU_k\tau_A) = \mathrm{tr}(P\tau_A) + \sum_{0 \leqslant j < k < d} (\rho_{kj} - \rho_{jk})\lambda\,\mathrm{tr}(PU_jU_k) = \mathrm{tr}(P\tau_A), \quad \text{(E5)}$$

which implies that $P\tau_A$ is majorized by $P\varrho_A$ given that $P\tau_A = \lambda P$ is proportional to a projector. As a corollary, τ_A is majorized by ϱ_A. By the same token τ_B is majorized by ϱ_B.

When $d \neq 4$, according to lemma 3 in the main text and lemma 6 below, the purity of ϱ_A can be computed as follows,

$$\mathrm{tr}(\varrho_A^2) = \mathrm{tr}(\tau_A^2) + \sum_{\substack{0 \leqslant j < k < d \\ 0 \leqslant j' < k' < d}} (\rho_{kj} - \rho_{jk})(\rho_{k'j'} - \rho_{j'k'})\,\mathrm{tr}(U_jU_kU_{j'}U_{k'}\tau_A^2)$$

$$= \wp\left[1 - \sum_{0 \leqslant j < k < d} (\rho_{kj} - \rho_{jk})^2\right] = \wp[1 + \mathrm{tr}(\rho^2) - \mathrm{tr}(\rho\rho^{\mathrm{T}})] = \tfrac{1}{2}\wp(2 + \|\rho - \rho^{\mathrm{T}}\|_{\mathrm{HS}}^2), \quad \text{(E6)}$$

where $\wp = \mathrm{tr}(\tau_A^2) = \mathrm{tr}(\tau_B^2)$ is the masking purity. Here the last equality follows from the fact that

$$\|\rho - \rho^{\mathrm{T}}\|_{\mathrm{HS}}^2 = 2[\mathrm{tr}(\rho^2) - \mathrm{tr}(\rho\rho^{\mathrm{T}})]. \quad \text{(E7)}$$

By the same token we can deduce

$$\mathrm{tr}(\varrho_B^2) = \wp[1 + \mathrm{tr}(\rho^2) - \mathrm{tr}(\rho\rho^{\mathrm{T}})] = \tfrac{1}{2}\wp(2 + \|\rho - \rho^{\mathrm{T}}\|_{\mathrm{HS}}^2), \quad \text{(E8)}$$

which, together with Eq. (E6), confirms Eqs. (32) and (34).

Equation (33) is a corollary of Eq. (32) and the following equation:

$$\frac{4}{d}\mathscr{I}_{\mathrm{R}}(\rho)^2 \leqslant \|\rho - \rho^{\mathrm{T}}\|_{\mathrm{HS}}^2 \leqslant 2\mathscr{I}_{\mathrm{R}}(\rho)^2. \quad \text{(E9)}$$

Equation (E9) in turn follows from the equality $\mathscr{I}_{\mathrm{R}}(\rho) = \|\rho - \rho^{\mathrm{T}}\|_1/2$ in Eq. (31) [25] and the inequalities

$$\frac{1}{d}\|\rho - \rho^{\mathrm{T}}\|_1^2 \leqslant \|\rho - \rho^{\mathrm{T}}\|_{\mathrm{HS}}^2 \leqslant \frac{1}{2}\|\rho - \rho^{\mathrm{T}}\|_1^2. \quad \text{(E10)}$$

Here the first inequality is well known given that ρ is a density matrix on a Hilbert space of dimension d; the second inequality follows from the fact that $\rho - \rho^{\mathrm{T}}$ is hermitian and antisymmetric, which means its nonzero eigenvalues form pairs of opposite signs. Similarly, Eq. (35) is a corollary of Eqs. (34) and (E9).

When $d = 4$, according to lemmas 3 and 6, the purity of ϱ_A reads

$$\mathrm{tr}(\varrho_A^2) = \mathrm{tr}(\tau_A^2) + \sum_{\substack{0 \leqslant j < k < d \\ 0 \leqslant j' < k' < d}} (\rho_{kj} - \rho_{jk})(\rho_{k'j'} - \rho_{j'k'})\,\mathrm{tr}(U_jU_kU_{j'}U_{k'}\tau_A^2)$$

$$= \wp\left[1 - \sum_{0 \leqslant j < k \leqslant 3} (\rho_{kj} - \rho_{jk})^2\right] + \sum_{\substack{0 \leqslant j < k \leqslant 3 \\ 0 \leqslant j' < k' \leqslant 3}} (\delta_{j=0}\epsilon_{kj'k'} + \delta_{j'=0}\epsilon_{jkk'})(\rho_{kj} - \rho_{jk})(\rho_{k'j'} - \rho_{j'k'})\,\mathrm{tr}(U_1U_2U_3\tau_A^2)$$

$$= \wp[1 + \mathrm{tr}(\rho^2) - \mathrm{tr}(\rho\rho^{\mathrm{T}})] + \sum_{\substack{0 \leqslant j < k \leqslant 3 \\ 0 \leqslant j' < k' \leqslant 3}} (\delta_{j=0}\epsilon_{kj'k'} + \delta_{j'=0}\epsilon_{jkk'})(\rho_{kj} - \rho_{jk})(\rho_{k'j'} - \rho_{j'k'})\,\mathrm{tr}(U_1U_2U_3\tau_A^2). \quad \text{(E11)}$$

Similarly, the purity of ϱ_B reads

$$\mathrm{tr}(\varrho_B^2) = \wp[1 + \mathrm{tr}(\rho^2) - \mathrm{tr}(\rho\rho^{\mathrm{T}})] + \sum_{\substack{0 \leqslant j < k \leqslant 3 \\ 0 \leqslant j' < k' \leqslant 3}} (\delta_{j=0}\epsilon_{kj'k'} + \delta_{j'=0}\epsilon_{jkk'})(\rho_{kj} - \rho_{jk})(\rho_{k'j'} - \rho_{j'k'})\,\mathrm{tr}(V_1V_2V_3\tau_B^2)$$

$$= \wp[1 + \mathrm{tr}(\rho^2) - \mathrm{tr}(\rho\rho^{\mathrm{T}})] - \sum_{\substack{0 \leqslant j < k \leqslant 3 \\ 0 \leqslant j' < k' \leqslant 3}} (\delta_{j=0}\epsilon_{kj'k'} + \delta_{j'=0}\epsilon_{jkk'})(\rho_{kj} - \rho_{jk})(\rho_{k'j'} - \rho_{j'k'})\,\mathrm{tr}(U_1U_2U_3\tau_A^2), \quad \text{(E12)}$$

which, together with Eq. (E11), implies Eq. (32). The second equality in Eq. (E12) is a consequence of the equality $\mathrm{tr}(V_1 V_2 V_3 \tau_B^2) = -\mathrm{tr}(U_1 U_2 U_3 \tau_A^2)$, which can be derived as follows. From Eq. (29) we can deduce that

$$(\mathbb{1}_A \otimes V_1 V_2 V_3)|\Psi_0\rangle = (U_3 U_2 U_1 \otimes \mathbb{1}_B)|\Psi_0\rangle, \tag{E13}$$

which implies that

$$\mathrm{tr}\big(V_1 V_2 V_3 \tau_B^2\big) = \mathrm{tr}\big(U_3 U_2 U_1 \tau_A^2\big) = -\mathrm{tr}\big(U_1 U_2 U_3 \tau_A^2\big). \tag{E14}$$

Here the first equality follows from lemma 7 below, and the second one follows from the fact that U_1, U_2, U_3 anticommute with each other.

Equation (33) is still a corollary of Eqs. (32) and (E9). This observation completes the proof of corollary 6. ∎

2. Two auxiliary lemmas

Lemma 6. Suppose M is the masker for $\mathscr{D}^{\mathrm{R}}(\mathcal{H})$ in theorem 3. Let $\rho \in \mathscr{D}(\mathcal{H})$, $\varrho = M(\rho)$, $\varrho_A = \mathrm{tr}_B(\varrho)$, and $\varrho_B = \mathrm{tr}_A(\varrho)$. Then

$$\varrho_A = \tau_A + \sum_{0 \leqslant j < k < d} (\rho_{kj} - \rho_{jk}) U_j U_k \tau_A, \tag{E15}$$

$$\varrho_B = \tau_B + \sum_{0 \leqslant j < k < d} (\rho_{kj} - \rho_{jk}) V_j V_k \tau_B, \tag{E16}$$

where $U_0 = \mathbb{1}_A$, $V_0 = \mathbb{1}_B$, and U_j, V_j for $j = 1, 2, \ldots, d-1$ are determined by Eq. (29).

Proof. By assumption we have

$$\varrho = M(\rho) = \sum_{j,k} \rho_{jk} M|j\rangle\langle k|M^\dagger = \sum_{j,k} \rho_{jk}|\Psi_j\rangle\langle\Psi_k|$$

$$= \sum_{j,k} \rho_{jk}(U_j \otimes \mathbb{1}_B)|\Psi_0\rangle\langle\Psi_0|(U_k^\dagger \otimes \mathbb{1}_B). \tag{E17}$$

Therefore

$$\varrho_A = \mathrm{tr}_B(\varrho) = \sum_{j,k} \rho_{jk} U_j \tau_A U_k^\dagger = \sum_{j,k} \rho_{jk} U_j U_k^\dagger \tau_A$$

$$= \tau_A + \sum_{j \neq k} \rho_{jk} U_j U_k^\dagger \tau_A$$

$$= \tau_A + \sum_{0 \leqslant j < k < d} (\rho_{kj} - \rho_{jk}) U_j U_k \tau_A. \tag{E18}$$

Here the third equality follows from the fact that U_k and $U_k^\dagger$ commute with τ_A. The last equality follows from the fact that $U_0 = \mathbb{1}_A$ and $\{U_j\}_{j=1}^{d-1}$ is a set of HR matrices on $\mathcal{H}_A$, which means

$$U_j U_k + U_k U_j = -2\delta_{jk} \mathbb{1}_A \quad \forall j, k = 1, 2, \ldots, d-1. \tag{E19}$$

Equation (E16) can be proved in a similar way. ∎

Lemma 7. Suppose $|\Psi_0\rangle$ is a bipartite ket in the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$ with reduced states $\tau_A = \mathrm{tr}_B(|\Psi_0\rangle\langle\Psi_0|)$ and $\tau_B = \mathrm{tr}_A(|\Psi_0\rangle\langle\Psi_0|)$. Suppose U and V are unitary operators on $\mathcal{H}_A$ and $\mathcal{H}_B$ that satisfy

$$(U \otimes \mathbb{1}_B)|\Psi_0\rangle = (\mathbb{1}_A \otimes V)|\Psi_0\rangle; \tag{E20}$$

then

$$\mathrm{tr}\big(\tau_A^\alpha U\big) = \mathrm{tr}\big(\tau_B^\alpha V\big) \quad \forall \alpha > 0. \tag{E21}$$

Suppose P_A and P_B are the projectors onto the eigenspaces of τ_A and τ_B, respectively, which are associated with a same

nonzero eigenvalue λ; then

$$\mathrm{tr}(P_A U) = \mathrm{tr}(P_B V). \tag{E22}$$

Proof. We first prove Eq. (E22). Equation (E20) implies that U commutes with τ_A and P_A, while V commutes with τ_B and P_B. In addition, by assumption we have

$$(P_A \otimes \mathbb{1}_B)|\Psi_0\rangle = (\mathbb{1}_A \otimes P_B)|\Psi_0\rangle, \tag{E23}$$

$$(P_A U \otimes \mathbb{1}_B)|\Psi_0\rangle = (P_A \otimes \mathbb{1}_B)(\mathbb{1}_A \otimes V)|\Psi_0\rangle$$
$$= (\mathbb{1}_A \otimes P_B V)|\Psi_0\rangle. \tag{E24}$$

Therefore

$$\lambda\mathrm{tr}(P_A U) = \mathrm{tr}(P_A U \tau_A) = \langle\Psi_0|(P_A U \otimes \mathbb{1}_B)|\Psi_0\rangle$$
$$= \langle\Psi_0|(\mathbb{1}_A \otimes P_B V)|\Psi_0\rangle = \mathrm{tr}(P_B V \tau_B) = \lambda\mathrm{tr}(P_B V), \tag{E25}$$

which implies Eq. (E22).

Equation (E21) is a corollary of Eq. (E22) given that τ_A and τ_B have the same nonzero spectrum. When $\alpha = 1$, Eq. (E21) can also be derived directly as follows:

$$\mathrm{tr}(\tau_A U) = \langle\Psi_0|(U \otimes \mathbb{1}_B)|\Psi_0\rangle = \langle\Psi_0|(\mathbb{1}_A \otimes V)|\Psi_0\rangle$$
$$= \mathrm{tr}(\tau_B V). \tag{E26}$$

∎

APPENDIX F: PROOF OF COROLLARY 7

Corollary 7. Let E be an entanglement monotone; then

$$E(\mathscr{D}^{\mathrm{R}}(\mathcal{H})) = E(\mathscr{P}^{\mathrm{R}}(\mathcal{H})) = E(|\Phi(\tilde{\kappa}(d))\rangle), \tag{38}$$

$$E^{\mathrm{R}}(\mathscr{D}^{\mathrm{R}}(\mathcal{H})) = E^{\mathrm{R}}(\mathscr{P}^{\mathrm{R}}(\mathcal{H})) = E(|\Phi(\kappa^{\mathrm{R}}(d))\rangle), \tag{39}$$

where $|\Phi(m)\rangle$ is a maximally entangled state of Schmidt rank m.

Proof of corollary 7. Any masker for $\mathscr{D}^{\mathrm{R}}(\mathcal{H})$ is a masker for $\mathscr{P}^{\mathrm{R}}(\mathcal{H})$ and vice versa, so $E(\mathscr{D}^{\mathrm{R}}(\mathcal{H})) = E(\mathscr{P}^{\mathrm{R}}(\mathcal{H}))$ according to lemma 1. Suppose $M : \mathcal{H} \mapsto \mathcal{H}_A \otimes \mathcal{H}_B$ is a masker for $\mathscr{D}^{\mathrm{R}}(\mathcal{H})$. Let $|\Psi_0\rangle = M|0\rangle$; then lemma 1 implies that

$$E(\mathscr{D}^{\mathrm{R}}(\mathcal{H})) = E(|\Psi_0\rangle\langle\Psi_0|) \geqslant E(|\Phi(\tilde{\kappa}(d))\rangle), \tag{F1}$$

where $\tilde{\kappa}(d) := \max\{\kappa(d), 2\}$ (cf. corollary 5). Here the inequality follows from the fact that the nonzero spectrum of $\mathrm{tr}_B(|\Psi_0\rangle\langle\Psi_0|)$ (that is, the masking spectrum of M) is majorized by the nonzero spectrum of $\mathrm{tr}_B(|\Phi(\tilde{\kappa}(d))\rangle\langle\Phi(\tilde{\kappa}(d))|)$ according to corollary 4, so $|\Psi_0\rangle$ can be turned into $|\Phi(\tilde{\kappa}(d))\rangle$

by LOCC according to the majorization criterion of Nielsen [47]. In addition, the inequality in Eq. (F1) can be saturated by choosing a suitable masker according to corollary 4. This observation confirms Eq. (38). Equation (39) can be proved using a similar reasoning. ∎

APPENDIX G: PROOFS OF THEOREMS 4 AND 5

Theorem 4. $\mathscr{D}^{\mathrm{R}}(\mathcal{H})$ is a maximal maskable set.

Proof of theorem 4. Let $\rho \in \mathscr{D}(\mathcal{H})$ be an arbitrary density matrix; suppose the set $\mathscr{D}^{\mathrm{R}}(\mathcal{H}) \cup \{\rho\}$ can be masked by the isometry $M : \mathcal{H} \mapsto \mathcal{H}_A \times \mathcal{H}_B$. Then M is also a maker for $\mathscr{D}^{\mathrm{R}}(\mathcal{H})$. Let τ_A and τ_B be the common reduced density matrices. Without loss of generality, we can assume that τ_A and τ_B have full rank. Let $\varrho = M(\rho)$, $\varrho_A = \mathrm{tr}_B(\varrho)$, and $\varrho_B = \mathrm{tr}_A(\varrho)$. Then we have $\varrho_A = \tau_A$ and $\varrho_B = \tau_B$, so that

$$\mathrm{tr}(\varrho_A^2) + \mathrm{tr}(\varrho_B^2) = \mathrm{tr}(\tau_A^2) + \mathrm{tr}(\tau_B^2) = 2\mathrm{tr}(\tau_A^2). \tag{G1}$$

When $d \geqslant 3$, in conjunction with corollary 6, this equation implies that $\mathrm{tr}(\rho\rho^{\mathrm{T}}) = \mathrm{tr}(\rho^2)$, so that $\rho \in \mathscr{D}^{\mathrm{R}}(\mathcal{H})$. Therefore $\mathscr{D}^{\mathrm{R}}(\mathcal{H})$ is a maximal maskable set.

When $d = 2$, the density matrix ϱ_A has the form

$$\varrho_A = \tau_A + (\rho_{10} - \rho_{01})U\tau_A \tag{G2}$$

according to lemma 6, where U is a unitary matrix that satisfies $U^2 = -\mathbb{1}_A$. So the equality $\varrho_A = \tau_A$ implies that $\rho_{10} = \rho_{01}$ and that $\rho \in \mathscr{D}^{\mathrm{R}}(\mathcal{H})$. Therefore $\mathscr{D}^{\mathrm{R}}(\mathcal{H})$ is a maximal maskable set. Alternatively, this conclusion follows from corollary 1 (cf. Refs. [16,17]). This observation completes the proof of theorem 4.

In the case of pure states, theorem 4 can be proved in a completely different way, which is less technical and more instructive. Let $|\psi\rangle$ be any ket in $\mathcal{H}$ that is not proportional to any real ket. Let $\mathscr{S}$ be the union of $\mathscr{P}^{\mathrm{R}}(\mathcal{H})$ and $\{|\psi\rangle\langle\psi|\}$. To prove that $\mathscr{P}^{\mathrm{R}}(\mathcal{H})$ is a maximal maskable set within $\mathscr{P}(\mathcal{H})$, it suffices to prove that $\mathscr{S}$ is not maskable.

By assumption $|\psi\rangle$ has the form $|\psi\rangle = c_1|\psi_1\rangle + \mathrm{i}c_2|\psi_2\rangle$, where $|\psi_1\rangle, |\psi_2\rangle$ are two real kets that are linearly independent, and c_1, c_2 are nonzero real coefficients that satisfy the normalization condition $c_1^2 + c_2^2 = 1$. Let $\mathcal{H}_2$ be the span of $\{|\psi_1\rangle, |\psi_2\rangle\}$ and let $\mathscr{S}_2$ be the set of all real pure states on $\mathcal{H}_2$. Then we have $|\psi\rangle \in \mathcal{H}_2$ and $\mathscr{S}_2 \cup \{|\psi\rangle\langle\psi|\} \subseteq \mathscr{S}$. Geometrically, $\mathscr{S}_2$ is a great circle on the Bloch sphere associated with $\mathcal{H}_2$, while $|\psi\rangle\langle\psi|$ is a point on the sphere, but not on this great circle. Therefore $\mathscr{S}_2 \cup \{|\psi\rangle\langle\psi|\}$ is not maskable according to corollary 1, which implies that $\mathscr{S}$ is not maskable. ∎

Theorem 5. Suppose $d \geqslant 3$ and $M : \mathcal{H} \mapsto \mathcal{H}_A \otimes \mathcal{H}_B$ is a masker for $\mathscr{D}^{\mathrm{R}}(\mathcal{H})$. Let $|\Psi_0\rangle = M|0\rangle$; then any state in $M(\mathscr{D}(\mathcal{H}))$ can be created from $|\Psi_0\rangle\langle\Psi_0|$ by local operations and classical communication (LOCC). In addition, $E(M(\rho)) \leqslant E(|\Psi_0\rangle\langle\Psi_0|)$ for any entanglement monotone E and all $\rho \in \mathscr{D}(\mathcal{H})$. When E is a convex strict monotone, the upper bound is saturated iff $\rho \in \mathscr{P}^{\mathrm{R}}(\mathcal{H})$.

Proof of theorem 5. Let $\tau_A = \mathrm{tr}_B(|\Psi_0\rangle\langle\Psi_0|)$. Let ρ be an arbitrary state in $\mathscr{D}(\mathcal{H})$, $\varrho = M(\rho)$, and $\varrho_A = \mathrm{tr}_B(\varrho)$. According to corollary 6, τ_A is majorized by ϱ_A. If ρ is pure, so that ϱ is also pure, then ϱ can be created from $|\Psi_0\rangle\langle\Psi_0|$ by LOCC according to the majorization criterion [47]. The same conclusion applies when ρ is mixed, in which case ρ can be

expressed as a convex mixture of pure states and so can ϱ accordingly.

By the above discussion, we have $E(\varrho) \leqslant E(|\Psi_0\rangle\langle\Psi_0|)$ for any entanglement monotone E since $|\Psi_0\rangle\langle\Psi_0|$ can be turned into ϱ by LOCC. Next, suppose E is a convex strict monotone. If ρ, ϱ are pure and the upper bound $E(\varrho) \leqslant E(|\Psi_0\rangle\langle\Psi_0|)$ is saturated, then ϱ and $|\Psi_0\rangle\langle\Psi_0|$ can be turned into each other by LOCC. Therefore $\varrho_A, \varrho_B, \tau_A$, and τ_B have the same nonzero spectrum according to the majorization criterion [47] and thus have the same purity. Now corollary 6 implies that ρ is a real density matrix, that is, $\rho \in \mathscr{P}^{\mathrm{R}}(\mathcal{H})$.

If ρ is mixed, then it can be expressed as a convex mixture of pure states $\rho = \sum_r a_r|\psi_r\rangle\langle\psi_r|$ with $a_r > 0$ and $|\psi_r\rangle\langle\psi_r| \notin \mathscr{P}^{\mathrm{R}}(\mathcal{H})$ for at least one r. Accordingly, we have $\varrho = \sum_r a_r M|\psi_r\rangle\langle\psi_r|M^\dagger$,

$$E(M|\psi_r\rangle\langle\psi_r|M^\dagger) \leqslant E(|\Psi_0\rangle\langle\Psi_0|) \quad \forall r, \tag{G3}$$

and the inequality is strict for at least one r. Therefore

$$E(\varrho) \leqslant \sum_r a_r E(M|\psi_r\rangle\langle\psi_r|M^\dagger) < E(|\Psi_0\rangle\langle\Psi_0|), \tag{G4}$$

so the inequality $E(\varrho) \leqslant E(|\Psi_0\rangle\langle\Psi_0|)$ cannot be saturated when ρ is mixed. This observation completes the proof of theorem 5. ∎

APPENDIX H: PROOFS OF PROPOSITIONS 3 AND 4

Proposition 3. Suppose $\mathscr{P}(\boldsymbol{c})$ with $d \geqslant 2$ is equivalent to a subset of $\mathscr{P}^{\mathrm{R}}(\mathcal{H}')$; then $d = 2$ and $c_0 = c_1 = 1/\sqrt{2}$.

Proof of proposition 3. Note that $\mathscr{P}(\boldsymbol{c})$ and $\mathscr{P}(\boldsymbol{c}')$ are equivalent whenever $\boldsymbol{c}'$ is a permutation of $\boldsymbol{c}$. So we can assume that $0 < c_0 \leqslant c_1 \leqslant \cdots \leqslant c_{d-1} < 1$ without loss of generality, which implies that $0 < c_0^2 \leqslant 1/d$. Let

$$|\psi_k\rangle = c_0 e^{2k\pi\mathrm{i}/3}|0\rangle + \sum_{j=1}^{d-1} c_j|j\rangle, \quad k = 0, 1, 2; \tag{H1}$$

then $|\psi_k\rangle \in \mathcal{K}(\boldsymbol{c})$ and $|\psi_k\rangle\langle\psi_k| \in \mathscr{P}(\boldsymbol{c})$. Suppose $\mathscr{P}(\boldsymbol{c})$ is equivalent to a subset of $\mathscr{P}^{\mathrm{R}}(\mathcal{H}')$; then the following triple product must be real,

$$\mathrm{tr}[(|\psi_0\rangle\langle\psi_0|)(|\psi_1\rangle\langle\psi_1|)(|\psi_2\rangle\langle\psi_2|)] = \left(c_0^2 e^{2\pi\mathrm{i}/3} + 1 - c_0^2\right)^3, \tag{H2}$$

since the triple product is invariant under isometry. In conjunction with the condition $0 < c_0^2 \leqslant 1/d \leqslant 1/2$, we can deduce that $d = 2$ and $c_0^2 = 1 - c_0^2$, which implies that $c_0 = c_1 = 1/\sqrt{2}$. This observation completes the proof of proposition 3. ∎

Proposition 4. Suppose $\mathscr{P}^{\mathrm{R}}(\mathcal{H}')$ with $\dim(\mathcal{H}') \geqslant 2$ is equivalent to a subset of $\mathscr{P}(\boldsymbol{c})$; then $\dim(\mathcal{H}') = 2$.

Proof of proposition 4. Suppose on the contrary that the set $\mathscr{P}^{\mathrm{R}}(\mathcal{H}')$ with $\dim(\mathcal{H}') \geqslant 3$ is equivalent to a subset of $\mathscr{P}(\boldsymbol{c})$ under the isometry S. Let $|\psi_k\rangle = S|k\rangle$ for $k = 0, 1, 2$;

then $|\psi_k\rangle$ have the form

$$|\psi_0\rangle = \sum_j c_j e^{i\alpha_j} |j\rangle, \tag{H3}$$

$$|\psi_1\rangle = \sum_j c_j e^{i\beta_j} |j\rangle, \tag{H4}$$

$$|\psi_2\rangle = \sum_j c_j e^{i\gamma_j} |j\rangle, \tag{H5}$$

where $0 \leqslant \alpha_j, \beta_j, \gamma_j < 2\pi$ for $j = 0, 1, \ldots, d-1$. Moreover, we can assume that $\alpha_j = 0$ for all j without loss of generality. Let

$$|\psi_{kl}\rangle = \frac{1}{\sqrt{2}} S(|k\rangle + |l\rangle), \quad 0 \leqslant k < l \leqslant 2; \tag{H6}$$

then $|\psi_{kl}\rangle \in \mathscr{K}(\boldsymbol{c})$ by assumption, which implies that

$$\left|\frac{1 + e^{i\beta_j}}{\sqrt{2}}\right|^2 = \left|\frac{1 + e^{i\gamma_j}}{\sqrt{2}}\right|^2 = \left|\frac{1 + e^{i(\beta_j - \gamma_j)}}{\sqrt{2}}\right|^2 = 1, \tag{H7}$$

$$\cos(\beta_j) = \cos(\gamma_j) = \cos(\beta_j - \gamma_j) = 0 \quad \forall j. \tag{H8}$$

However, the last equation can never hold. This contradiction shows that $\mathscr{P}^R(\mathcal{H}')$ cannot be equivalent to a subset of $\mathscr{P}(\boldsymbol{c})$ except when $\dim(\mathcal{H}') = 2$, which confirms proposition 4. ∎

[1] G. R. Blakley, Safeguarding cryptographic keys, in *Managing Requirements Knowledge, International Workshop on* (IEEE Computer Society, Los Alamitos, CA, USA, 1979), Vol. 1, p. 313.

[2] A. Shamir, How to share a secret, Commun. ACM **22**, 612 (1979).

[3] M. Hillery, V. Bužek, and A. Berthiaume, Quantum secret sharing, Phys. Rev. A **59**, 1829 (1999).

[4] R. Cleve, D. Gottesman, and H.-K. Lo, How to Share a Quantum Secret, Phys. Rev. Lett. **83**, 648 (1999).

[5] D. P. DiVincenzo, D. Leung, and B. Terhal, Quantum data hiding, IEEE Trans. Inf. Theory **48**, 580 (2002).

[6] D. N. Page, Average Entropy of a Subsystem, Phys. Rev. Lett. **71**, 1291 (1993).

[7] P. Hayden and J. Preskill, Black holes as mirrors: quantum information in random subsystems, J. High Energy Phys. 09 (2007) 120.

[8] Y. Sekino and L. Susskind, Fast scramblers, J. High Energy Phys. 10 (2008) 065.

[9] Z.-W. Liu, S. Lloyd, E. Zhu, and H. Zhu, Entanglement, quantum randomness, and complexity beyond scrambling, J. High Energy Phys. 07 (2018), 041.

[10] S. L. Braunstein and A. K. Pati, Quantum Information Cannot be Completely Hidden in Correlations: Implications for the Black-Hole Information Paradox, Phys. Rev. Lett. **98**, 080502 (2007).

[11] K. Modi, A. K. Pati, A. Sen(De), and U. Sen, Masking Quantum Information is Impossible, Phys. Rev. Lett. **120**, 230501 (2018).

[12] W. K. Wootters and W. H. Zurek, A single quantum cannot be cloned, Nature (London) **299**, 802 (1982).

[13] D. Dieks, Communication by EPR devices, Phys. Lett. A **92**, 271 (1982).

[14] A. Lamas-Linares, C. Simon, J. C. Howell, and D. Bouwmeester, Experimental quantum cloning of single photons, Science **296**, 712 (2002).

[15] H. Barnum, C. M. Caves, C. A. Fuchs, R. Jozsa, and B. Schumacher, Noncommuting Mixed States Cannot be Broadcast, Phys. Rev. Lett. **76**, 2818 (1996).

[16] X.-B. Liang, B. Li, and S.-M. Fei, Complete characterization of qubit masking, Phys. Rev. A **100**, 030304(R) (2019).

[17] F. Ding and X. Hu, Masking quantum information on hyperdisks, Phys. Rev. A **102**, 042404 (2020).

[18] H. Cao, Y. Du, Z. Guo, K. Han, and C. Yang, Masking quantum information encoded in pure and mixed states, arXiv:2004.14572.

[19] H. Araki, On a characterization of the state space of quantum mechanics, Commun. Math. Phys. **75**, 1 (1980).

[20] M. McKague, M. Mosca, and N. Gisin, Simulating Quantum Systems Using Real Hilbert Spaces, Phys. Rev. Lett. **102**, 020505 (2009).

[21] L. Hardy and W. K. Wootters, Limited holism and real-vector-space quantum theory, Found. Phys. **42**, 454 (2012).

[22] J. C. Baez, Division algebras and quantum theory, Found. Phys. **42**, 819 (2012).

[23] M.-O. Renou, D. Trillo, M. Weilenmann, L. P. Thinh, A. Tavakoli, N. Gisin, A. Acin, and M. Navascues, Quantum physics needs complex numbers, arXiv:2101.10873.

[24] A. Hickey and G. Gour, Quantifying the imaginarity of quantum mechanics, J. Phys. A: Math. Theor. **51**, 414009 (2018).

[25] K.-D. Wu, T. V. Kondra, S. Rana, C. M. Scandolo, G.-Y. Xiang, C.-F. Li, G.-C. Guo, and A. Streltsov, Operational Resource Theory of Imaginarity, Phys. Rev. Lett. **126**, 090401 (2021).

[26] X.-B. Liang, B. Li, S.-M. Fei, and H. Fan, Impossibility of masking a set of quantum states of nonzero measure, Phys. Rev. A **101**, 042321 (2020).

[27] A. Hurwitz, Über die Komposition der quadratischen Formen, Math. Ann. **88**, 1 (1923).

[28] J. Radon, Lineare Scharen orthogonaler Matrizen, Abh. Math. Sem. Hamburg **1**, 1 (1922).

[29] B. Eckmann, Hurwitz-Radon matrices revisited: From effective solution of the Hurwitz matrix equations to Bott periodicity, in *Mathematical Survey Lectures 1943–2004* (Springer, Berlin, 2006), pp. 141–153.

[30] S. Hill and W. K. Wootters, Entanglement of a Pair of Quantum Bits, Phys. Rev. Lett. **78**, 5022 (1997).

[31] W. K. Wootters, Entanglement of Formation of an Arbitrary State of Two Qubits, Phys. Rev. Lett. **80**, 2245 (1998).

[32] P. Rungta, V. Bužek, C. M. Caves, M. Hillery, and G. J. Milburn, Universal state inversion and concurrence in arbitrary dimensions, Phys. Rev. A **64**, 042315 (2001).

[33] W. K. Wootters, Quantum mechanics without probability amplitudes, Found. Phys. **16**, 391 (1986).

[34] L. Hardy, Quantum Theory From Five Reasonable Axioms, arXiv:quant-ph/0101012.

[35] G. Chiribella, G. M. D'Ariano, and P. Perinotti, Informational derivation of quantum theory, Phys. Rev. A **84**, 012311 (2011).

[36] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Quantum entanglement, Rev. Mod. Phys. **81**, 865 (2009).

[37] E. Prugovečki, Information-theoretical aspects of quantum measurement, Int. J. Theor. Phys. **16**, 321 (1977).

[38] A. J. Scott, Tight informationally complete quantum measurements, J. Phys. A: Math. Gen. **39**, 13507 (2006).

[39] H. Zhu and B.-G. Englert, Quantum state tomography with fully symmetric measurements and product measurements, Phys. Rev. A **84**, 022327 (2011).

[40] G. Zauner, Quantum designs: Foundations of a noncommutative design theory, Int. J. Quantum Inf. **09**, 445 (2011).

[41] J. M. Renes, R. Blume-Kohout, A. J. Scott, and C. M. Caves, Symmetric informationally complete quantum measurements, J. Math. Phys. **45**, 2171 (2004).

[42] C. A. Fuchs, M. C. Hoang, and B. C. Stacey, The SIC question: History and state of play, Axioms **6**, 21 (2017).

[43] I. D. Ivanović, Geometrical description of quantal state determination, J. Phys. A: Math. Gen. **14**, 3241 (1981).

[44] W. K. Wootters and B. D. Fields, Optimal state–determination by mutually unbiased measurements, Ann. Phys. **191**, 363 (1989).

[45] T. Durt, B.-G. Englert, I. Bengtsson, and K. Życzkowski, On mutually unbiased bases, Int. J. Quantum Inf. **08**, 535 (2010).

[46] P. Lounesto, *Clifford Algebras and Spinors*, London Mathematical Society Lecture Note Series Vol. 286 (Cambridge University Press, Cambridge, 2001).

[47] M. A. Nielsen, Conditions for a Class of Entanglement Transformations, Phys. Rev. Lett. **83**, 436 (1999).