Entropic uncertainty relations for general symmetric informationally complete positive operator-valued measures and mutually unbiased measurements

Shan Huang [1,2] Zeng-Bing Chen,[1,*] and Shengjun Wu [1,2,†]
[1]*School of Physics, Nanjing University, Nanjing 210093, China*
[2]*Institute for Brain Sciences and Kuang Yaming Honors School, Nanjing University, Nanjing 210023, China*

(Received 3 November 2020; revised 19 March 2021; accepted 22 March 2021; published 6 April 2021)

We construct inequalities between Rényi α-entropy and the indexes of coincidence of probability distributions, based on which we obtain improved state-dependent entropic uncertainty relations for general symmetric informationally complete positive operator-valued measures (SIC-POVMs) and mutually unbiased measurements (MUMs). We show that our uncertainty relations for general SIC-POVMs and MUMs can be tight for sufficiently mixed states, and, moreover, comparisons to the numerically optimal results are made via information diagrams.

DOI: 10.1103/PhysRevA.103.042205

I. INTRODUCTION

Incompatible observables cannot be measured with certainty simultaneously, though contrary to the general cognition of the physical world based on macroscopic experience, this is a fundamental element of quantum mechanics. Heisenberg made the first statement of this kind of uncertainty of quantum mechanics [1], and formulated the first uncertainty relation

$$\Delta P \Delta Q \geqslant \frac{\hbar}{2}, \tag{1}$$

where ΔP and ΔQ denote the standard deviation of momentum and position along the same direction, respectively. Robertson generalized it to two arbitrary observables [2]

$$\Delta X \Delta Y \geqslant \tfrac{1}{2}|\langle\psi|[X,Y]|\psi\rangle|, \tag{2}$$

where $[X,Y]$ denotes the commutator between X and Y.

Though clear and elegant enough, the standard deviation way of measuring uncertainty sometimes can be quite strange [3–5] and it turns out to be inappropriate in applications of information theory. On the other hand, entropy is found to be a more universal and effective measure of uncertainty [3,6–8], and entropic uncertainty relations (EURs) have many applications in quantum information theory. The lower bound on conditional min-entropy can characterize how much randomness one can extract from a source [9], and moreover, as entanglement between two systems reduces the uncertainty (lower bound on entropy) of measurements performed on one system provided that the other one is accessible, EURs are useful in entanglement witnessing [10–12]. EURs are also important in the security proof of quantum cryptography as they measure how much information is possibly leaked to an eavesdropper [13,14]. (See more applications in the review [15] and references therein.)

Any projective measurement made in one base cannot reveal any information stored in bases that are mutually unbiased to it, and this property endows mutually unbiased bases (MUBs) with a special role in quantum information theory. Based on the work of Deutsch [3] and Kraus [16], Maassen and Uffink proved the famous tight state-independent uncertainty relation for two MUBs in terms of Shannon entropy [17], and a generalization to multiple MUBs has also been explored [18–23]. However, an analytic construction of more than three MUBs in general dimensions has not yet been found, and the existence of complete MUBs in non-prime-power-dimensional spaces such as $d = 6$ is still an open question [24].

While general symmetric informationally complete positive operator-valued measures (SIC-POVMs) [25] and mutually unbiased measurements (MUMs) [26] are positive operator-valued measures with interesting properties similar to MUBs, and a complete set of them can be constructed analytically in all dimensions [26,27], uncertainty relations have been naturally generalized to take into consideration more generalized measurements [28–31] like them. In two recent works EURs are also constructed from quantum designs [32,33]. In this paper, we focus on uncertainty relations for SIC-POVMs and MUMs and deal with them under a unified framework.

This paper is structured as follows. In Sec. II we introduce some necessary notations and review the concepts of entropy, SIC-POVM, and MUM. In Sec. III we propose entropic uncertainty relations for general SIC-POVMs, and in Sec. IV uncertainty relations for MUMs are constructed. In Sec. V, we make further discussions and draw a brief conclusion.

II. PRELIMINARIES

A positive operator-valued measure (POVM) $\mathcal{P}$ on a d-dimensional Hilbert space $\mathcal{H}_d$ consists of a set of positive semidefinite operators that sum up to the identity $\mathcal{P} = \{P_i | P_i \geqslant 0, \sum_i P_i = \mathbf{1}_d\}$. The probability distribution induced by performing a POVM measurement $\mathcal{P}$ on a quantum state ρ is denoted by $\mathscr{P} = (p_1, p_2, \ldots)$, where $p_i = \mathrm{Tr}(P_i\rho)$ is the probability of obtaining the ith result; the corresponding index of coincidence is defined as the sum of the squares of the

*zbchen@nju.edu.cn
†sjwu@nju.edu.cn

TABLE I. Notations and meaning.

1.	ρ	Density matrix
2.	L	The length of a probability distribution
3.	$\mathcal{H}_d$	d-dimensional Hilbert space
4.	$\mathbf{1}_d$	d-dimensional identity matrix
5.	$\mathbf{P}$	A boldfaced letter is, if not specified otherwise, a finite set of POVMs
6.	$\mathscr{P}$	A probability distribution
7.	$I(\mathscr{P})$	Index of coincidence of $\mathscr{P}$
8.	$I(\mathbf{P}\|\rho)$	The sum of indexes of coincidence induced by performing $\mathbf{P}$ on ρ
9.	$H_\alpha(\mathbf{P}\|\rho)$	Sum of Rényi α entropies for the measurements $\mathbf{P}$ performed on ρ
10.	$\mathscr{P}_x^L[c]$, $\mathscr{P}_y^L[c]$	Defined in Eqs. (10) and (11), two probability distributions over L outcomes, $I(\mathscr{P}_x^L[c]) = I(\mathscr{P}_y^L[c]) = c$

probabilities, i.e.,

$$I(\mathcal{P}|\rho) = I(\mathscr{P}) = \sum_i p_i^2. \tag{3}$$

The Shannon entropy of $\mathscr{P}$, defined by $H(\mathscr{P}) = H(\mathcal{P}|\rho) = -\sum_{i=1}^d p_i \log_2 p_i$, gives a measure of the uncertainty for the measurement outcomes. Rényi generalized it to a family of entropies [34]

$$H_\alpha(\mathcal{P}|\rho) = \frac{1}{1-\alpha}\log_2\left(\sum_{i=1} p_i^\alpha\right) \quad (\alpha > 0,\ \alpha \neq 1),$$

which reduces to Shannon entropy in the limitation $\lim_{\alpha\to 1} H_\alpha(\mathcal{P}|\rho) = H_1(\mathcal{P}|\rho) = H(\mathcal{P}|\rho)$. Following Ref. [35], we call the range of the map $\mathscr{P} \to [I(\mathscr{P}), H_\alpha(\mathscr{P})]$ *information diagrams*.

For any finite set of POVMs $\mathbf{P} = \{\mathcal{P}^1, \mathcal{P}^2, \ldots\}$ performed on ρ, we consider the sum of indexes of coincidence

$$I(\mathbf{P}|\rho) = \sum_{m=1}^{|\mathbf{P}|} I(\mathcal{P}^m|\rho), \tag{4}$$

and the sum of entropies $H_\alpha(\mathbf{P}|\rho) = \sum_m H_\alpha(\mathcal{P}^m|\rho)$.

Table I contains some notations that are frequently used in this paper.

A. Symmetric informationally complete POVM

A POVM on $\mathcal{H}_d$ is said to be symmetric informationally complete (SIC-POVM) [25] if it consists of d^2 rank-1 operators $\mathbf{S} = \{S_i\}$ such that $\mathrm{Tr}(S_iS_j) = \frac{d\delta_{ij}+1}{d^2(d+1)}$. From the geometric point of view, with $S_i = \frac{1}{d}|\phi_i\rangle\langle\phi_i|$, SIC-POVM comprises d^2 subnormalized equiangular vectors $\{\frac{1}{d}|\phi_i\rangle\}$ in C^d as $|\langle\phi_i|\phi_j\rangle|^2 = \frac{d\delta_{ij}+1}{d+1}$ and $\sum_{i=1}^{d^2}\frac{1}{d}|\phi_i\rangle\langle\phi_i| = \mathbf{1}_d$. Although research is still ongoing to prove or disprove the existence of SIC-POVM for general d, analytic and numerical results confirmed its existence for dimensions up to 67 [36].

SIC-POVM is informationally complete, as when performed on a system the resulting probability distributions fully reveal all the information of the corresponding density matrix. More concretely, any density matrix ρ can be constructed from the probabilities $\{p_j\}$ induced by SIC-POVM, and with $\mathrm{Tr}(\rho S_j) = p_j$ there is $\rho = \sum_j p_j[d(d+1)S_j - \mathbf{1}_d]$ [29].

By generalizing the method proposed in Ref. [23], Rastegin obtained [28]

$$I(\mathbf{S}|\rho) = \sum_{i=1}^{d^2} p_i^2 = \frac{1+\mathrm{Tr}(\rho^2)}{d(d+1)}, \tag{5}$$

where $p_i = \mathrm{Tr}(\rho S_i)$.

Generalizations of SIC-POVM to that with elements of any rank have been explored in Refs. [37,38], and in Ref. [27] the authors proved the existence of general SIC-POVMs in all dimensions by giving the explicit construction. Any general SIC-POVM $\mathbf{S}_g = \{S_i\}$ $(i = 1, 2, \ldots, d^2)$ is a POVM satisfying

$$\mathrm{Tr}(S_iS_i) = a \quad (\forall i,\ 1/d^3 < a \leqslant 1/d^2),$$
$$\mathrm{Tr}(S_iS_j) = \frac{1-ad}{d(d^2-1)} \quad (\forall i \neq j).$$

It is shown in Ref. [29] that

$$I(\mathbf{S}_g|\rho) = \frac{(ad^3-1)\mathrm{Tr}(\rho^2) + d(1-ad)}{d(d^2-1)}. \tag{6}$$

B. Mutually unbiased measurements

We say two orthonormal bases $\{|b_i^1\rangle\}$ and $\{|b_j^2\rangle\}$ $(1 \leqslant i, j \leqslant d)$ in $\mathcal{H}_d$ are mutually unbiased bases (MUBs) [39–42] if the inner products between their basis vectors satisfy $|\langle b_i^1|b_j^2\rangle| = \frac{1}{\sqrt{d}}$ $(\forall 1 \leqslant i, j \leqslant d)$. For any $d \geqslant 2$, one can find at least three MUBs and at most $d+1$ MUBs (an informationally complete set of MUBs). A complete set of MUBs can always be found if d is the power of a prime number, while the maximal number of MUBs in general is still an open question [24].

According to Ref. [23], for a set $\mathbf{B}$ of MUBs in $\mathcal{H}_d$,

$$I(\mathbf{B}|\rho) \leqslant \mathrm{Tr}(\rho^2) + \frac{|\mathbf{B}|-1}{d}. \tag{7}$$

Introduced as generalizations of MUBs, mutually unbiased measurements (MUMs) [26] are a set of POVMs $\mathbf{P} = \{\mathcal{P}^1, \mathcal{P}^2, \ldots\}$ with each $\mathcal{P}^m$ containing d elements $\mathcal{P}^m = \{P_1^m, \ldots, P_d^m\}$ and satisfying

$$\mathrm{Tr}\left(P_i^m\right) = 1,$$
$$\mathrm{Tr}\left(P_i^m P_j^{m'}\right) = \kappa\delta_{ij}\delta_{mm'} + (1-\delta_{ij})\delta_{mm'}\frac{1-\kappa}{d-1} + (1-\delta_{mm'})\frac{1}{d},$$

where κ $(\frac{1}{d} < \kappa \leqslant 1)$ is called the efficiency parameter. Note that the case $\kappa = 1$ corresponds with projective measurements consisting of mutually unbiased bases.

For any set $\mathbf{P}$ of MUMs on $\mathcal{H}_d$ there is [26,30]

$$I(\mathbf{P}|\rho) \leqslant \frac{|\mathbf{P}|}{d} + \frac{\kappa d - 1}{d(d-1)}[d\,\mathrm{Tr}(\rho^2) - 1], \tag{8}$$

and if $\mathbf{P}$ is complete,

$$I(\mathbf{P}|\rho) = \frac{d+1}{d} + \frac{\kappa d - 1}{d(d-1)}[d\,\mathrm{Tr}(\rho^2) - 1]. \tag{9}$$

III. UNCERTAINTY RELATIONS FOR GENERAL SIC-POVMs

In the following discussions we always arrange the probabilities in a probability distribution in descending order and ignore the probabilities being zero as they do not contribute to entropy, and we will frequently consider the two kinds of distributions described below. For any integer $L \geqslant 2$ and $\forall c \in [\frac{1}{L}, 1]$, $\mathscr{P}_x^L[c]$ and $\mathscr{P}_y^L[c]$ are two probability distributions over L outcomes, the indexes of coincidence of which are both c:

$$\mathscr{P}_x^L[c] = \left(\frac{1+\sqrt{(Lc-1)(L-1)}}{L}, (L-1)\odot\frac{1-\sqrt{(Lc-1)/(L-1)}}{L}\right), \quad I\big(\mathscr{P}_x^L[c]\big) = c, \tag{10}$$

$$\mathscr{P}_y^L[c] = \left((\lceil 1/c\rceil - 1)\odot\frac{1+\sqrt{(\lceil\frac{1}{c}\rceil c-1)/(\lceil\frac{1}{c}\rceil-1)}}{\lceil\frac{1}{c}\rceil}, \frac{1-\sqrt{(\lceil\frac{1}{c}\rceil c-1)(\lceil\frac{1}{c}\rceil-1)}}{\lceil\frac{1}{c}\rceil}\right), \quad I\big(\mathscr{P}_y^L[c]\big) = c, \tag{11}$$

where $\lceil\frac{1}{c}\rceil$ is the smallest integer that $\geqslant\frac{1}{c}$ and $l\odot p$ is shorthand for l probabilities being p. Note here the number of nonzero probabilities in $\mathscr{P}_y^L[c]$ is $L, L-1, \ldots$, respectively, when $c \in [\frac{1}{L}, \frac{1}{L-1}), [\frac{1}{L-1}, \frac{1}{L-2}), \ldots$, i.e., $\lceil 1/c\rceil$. Two examples of distributions over 4 outcomes are presented in Fig. 1.

We show in Appendix A the following theorem.

Theorem 1. For any discrete probability distribution $\mathscr{P}$ over L outcomes there is $H_\alpha(\mathscr{P}_y^L[I(\mathscr{P})]) \leqslant H_\alpha(\mathscr{P}) \leqslant H_\alpha(\mathscr{P}_x^L[I(\mathscr{P})])$ for $\alpha \in (0, 2]$, and $H_\alpha(\mathscr{P}_x^L[I(\mathscr{P})]) \leqslant H_\alpha(\mathscr{P}) \leqslant H_\alpha(\mathscr{P}_y^L[I(\mathscr{P})])$ for $\alpha \in [2, +\infty)$, where $H_\alpha(\mathscr{P})$ is the Rényi α-entropy of $\mathscr{P}$ and $I(\mathscr{P})$ is the index of coincidence of $\mathscr{P}$.

Thus $H_\alpha(\mathscr{P}_x^L[c])$ and $H_\alpha(\mathscr{P}_y^L[c])$ are boundary curves of the diagram of $I(\mathscr{P})$-$H_\alpha(\mathscr{P})$. The case $L = 4$ is shown in Fig. 2 as an example. The gray (thick) solid line is the graph of $H_2(\mathscr{P}) = -\log_2[I(\mathscr{P})]$. The upper bound (UB) on Shannon entropy (blue dashed line) and the lower bound (LB) on Rényi 5-entropy (orange dashed-dotted line) are respectively given by $H(\mathscr{P}_x^4[c])$ and $H_5(\mathscr{P}_x^4[c])$. At the same time, the lower bound on Shannon entropy (blue solid line) and the upper bound on Rényi 5-entropy (red dotted line) are respectively given by $H(\mathscr{P}_y^4[c])$ and $H_5(\mathscr{P}_y^4[c])$.

We should emphasize that Theorem 1 is a generalization of the Shannon entropic bounds obtained earlier in Refs. [19,35] to Rényi entropy. With Theorem 1 we immediately have the Rényi α-entropy $H_\alpha(\mathbf{S}_g|\rho)$ for performing any general SIC-POVMs with parameter a on $\mathcal{H}_d$ would satisfy

$$(2-\alpha)H_\alpha(\mathbf{S}_g|\rho) \leqslant (2-\alpha)H_\alpha\big(\mathscr{P}_x^{d^2}[I(\mathbf{S}_g|\rho)]\big), \tag{12}$$

$$(2-\alpha)H_\alpha(\mathbf{S}_g|\rho) \geqslant (2-\alpha)H_\alpha\big(\mathscr{P}_y^{d^2}[I(\mathbf{S}_g|\rho)]\big), \tag{13}$$

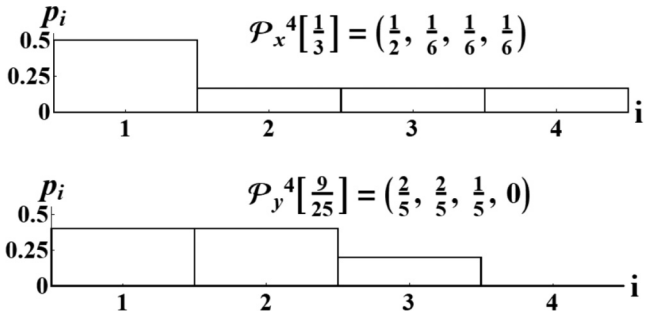

FIG. 1. Illustrations of distributions over four outcomes.

where $I(\mathbf{S}_g|\rho)$ is given by (6). This is the best result that can be obtained based on (6) only, hence uncertainty relations constructed from (6) such as those proposed in Refs. [28,29] cannot be stronger than our results. In the case $\alpha \to \infty$, Eq. (12) reduces to the result proposed previously by Rastegin [29],

$$H_\infty(\mathbf{S}_g|\rho) \geqslant 2\log_2 d - \log_2[1+\sqrt{ad^3-1}\sqrt{\mathrm{Tr}(\rho^2)d-1}]. \tag{14}$$

Now we show (12) and (13) are tight, respectively, when $\mathrm{Tr}(\rho^2) \in [\frac{1}{d}, d^2a]$ and $\mathrm{Tr}(\rho^2) \in [\frac{1}{d}, \frac{d-2+ad^2}{(d-1)^2}]$. We only need to show the probability distributions $\mathscr{P}_{y/x}^{d^2}[I(\mathbf{S}_g|\rho)]$ can be achieved by some positive semidefinite matrix in the form $\rho = \sum_i x_i S_i$, where $x_i = \frac{d(da-1)+d(d^2-1)p_i}{d^3a-1}$ is the solution to $\mathrm{Tr}(\rho) = 1$ and $\mathrm{Tr}(\rho S_i) = p_i \in \mathscr{P}_{y/x}^{d^2}[I(\mathbf{S}_g|\rho)]$. For (12), when $\mathrm{Tr}(\rho^2) \leqslant d^2a$, we have $x_1 \geqslant x_2 = \cdots = x_{d^2} \geqslant 0$, obviously $\rho \geqslant 0$. As for (13), we have $x_1 = \cdots = x_{d^2-1} \geqslant x_{d^2}$, as $\sum_i S_i = \mathbf{1}_d$, then $\forall|\phi\rangle \in \mathcal{H}_d$, $\langle\phi|\rho|\phi\rangle = \langle\phi|\sum_i x_i S_i|\phi\rangle = x_1 + (x_{d^2} - x_1)\mathrm{Tr}(S_{d^2}|\phi\rangle\langle\phi|) \geqslant x_1 + (x_{d^2} - x_1)/d \geqslant 0$, thus ρ is a density matrix.

By random sampling over density matrices on $\mathcal{H}_3$, we obtain the information diagram shown in Fig. 3. It is not a surprise to see that our entropic lower bound for SIC-POVM is not tight when $\mathrm{Tr}(\rho^2) > \frac{1}{2}$ since (12) and (13) are based on Eq. (6) only. Interestingly, the corresponding tight bound

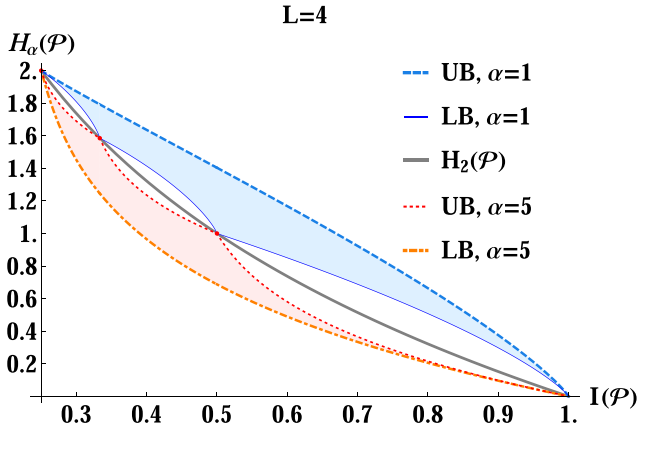

FIG. 2. Information diagrams of Shannon entropy and Rényi 5 entropy (see also Refs. [19,35]).

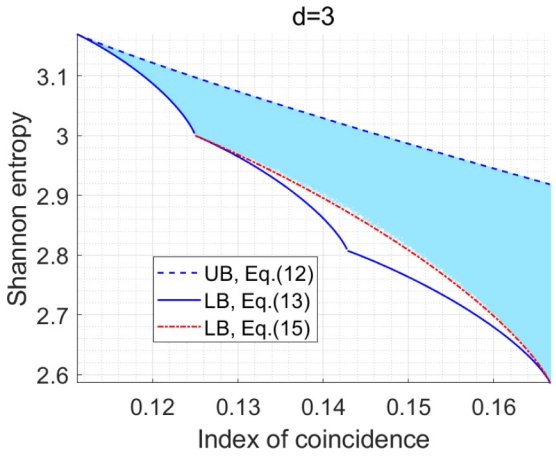

FIG. 3. Information diagram of Shannon entropy for SIC-POVM on $\mathcal{H}_3$ (cyan region).

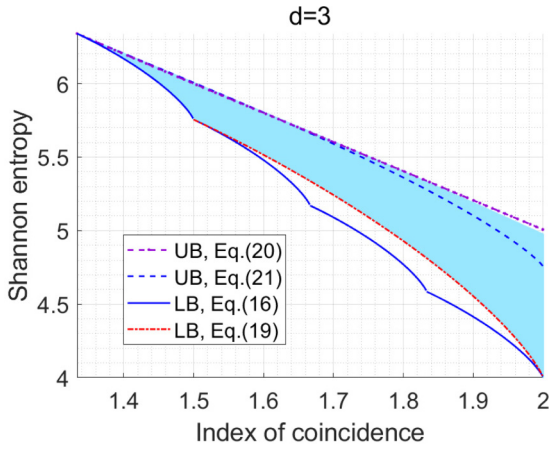

FIG. 4. Information diagram of Shannon entropy for complete MUBs in $\mathcal{H}_3$.

agrees with

$$H(\mathbf{S}_g|\rho) \geqslant H\big(\mathscr{P}_y^4[2I(\mathbf{S}_g|\rho)]\big) + 1. \tag{15}$$

IV. UNCERTAINTY RELATIONS FOR MUMs

A. Rényi entropy with $\alpha \leqslant 1$

We show Theorem 2 in Appendix C.

Theorem 2. The sum of Shannon entropies for a finite set $\mathbf{P}$ of $|\mathbf{P}|$ MUMs with efficiency parameter κ and performed on an arbitrary d-dimensional system ρ is bounded from below by

$$H\big(\mathscr{P}_y^d[c]\big) + k\log_2 n + (|\mathbf{P}| - k - 1)\log_2(n+1), \tag{16}$$

with $C(\mathbf{P}|\rho)=\frac{|\mathbf{P}|}{d} + \frac{\kappa d-1}{d(d-1)}[d\,\mathrm{Tr}(\rho^2) - 1]$, where $n = \lfloor \frac{|\mathbf{P}|}{C(\mathbf{P}|\rho)} \rfloor$, $k=\lfloor [C(\mathbf{P}|\rho) - \frac{M}{n+1}](n+1)n \rfloor$, and $c=C(\mathbf{P}|\rho) - \frac{k}{n} - \frac{|\mathbf{P}|-k-1}{n+1}$. Despite the complex expression, this theorem can be understood in a simple way as is discussed in Appendix C. When $\mathrm{Tr}(\rho^2) \in [\frac{1}{d}, \frac{d+\kappa-2}{(d-1)^2}]$, (16) reduces to

$$(|\mathbf{P}| - 1)\log_2 d + H\big(\mathscr{P}_y^d[C(\mathbf{P}|\rho) - (|\mathbf{P}| - 1)/d]\big), \tag{17}$$

which is actually valid for arbitrary Rényi α-entropy with $0 < \alpha \leqslant 1$, and quite similar to (12) it is tight.

We can linearize the first term of Eq. (16) based on its concavity with respect to c as follows, $H(\mathscr{P}_y^d[c]) \geqslant H(\mathscr{P}_y^d[\frac{1}{n+1}]) + n(n+1)(c - \frac{1}{n+1})[H(\mathscr{P}_y^d[\frac{1}{n}]) - H(\mathscr{P}_y^d[\frac{1}{n+1}])]$, which would then reduce to the result of Wu *et al.* [23] for MUBs,

$$\begin{aligned} H(\mathbf{B}|\rho) \geqslant & [|\mathbf{B}| - nC(\mathbf{B}|\rho)](n+1)\log_2(n+1) \\ & -[|\mathbf{B}| - (n+1)C(\mathbf{B}|\rho)]n\log_2 n, \end{aligned} \tag{18}$$

where $C(\mathbf{B}|\rho)$ is given by the right-hand side of (7) and $n = \lfloor \frac{|\mathbf{B}|}{C(\mathbf{B}|\rho)} \rfloor$. (16) is generally improved from (18) and they are equivalent only when $c = \frac{1}{n}$ or $\frac{1}{n+1}$.

As can be seen in Fig. 4, similar to (13), (16) is not tight when $\mathrm{Tr}(\rho^2) > \frac{1}{2}$ for $d = 3$ and the tight lower bound seems to be

$$H(\mathbf{B}|\rho) \geqslant 1 + 3H\left(\mathscr{P}_y^3\left[\frac{1 + \mathrm{Tr}(\rho^2)}{3}\right]\right). \tag{19}$$

As for the upper bound, with $L = d$ we only propose the following two unproved approximations,

$$(d+1)H\big(\mathscr{P}_x^d[I(\mathbf{B}|\rho)/(d+1)]\big), \quad \mathrm{Tr}(\rho^2) \approx 1, \tag{20}$$

$$d\log_2 d + H\big(\mathscr{P}_x^d[I(\mathbf{B}|\rho) - 1]\big), \quad \mathrm{Tr}(\rho^2) \approx \frac{1}{d}. \tag{21}$$

B. Rényi entropy with $\alpha \geqslant 2$

Theorem 3. Let $\mathbf{P}$ be a set of mutually unbiased measurements performed on a d-dimensional system ρ, then for any $\alpha \geqslant 2$,

$$\begin{aligned} \frac{1}{|\mathbf{P}|}H_\alpha(\mathbf{P}|\rho) \geqslant & \frac{\alpha}{1-\alpha}\log_2 p_a + \frac{\log_2 d}{(1-\alpha)\ln\left[1 + (d-1)^{\frac{2}{\alpha}}\right]} \\ & \times \ln\left[1 + (d-1)^{\frac{2}{\alpha}}\frac{p_b^2}{p_a^2}\right], \end{aligned} \tag{22}$$

where $p_a = \frac{1+\sqrt{(d-1)(dc-1)}}{d}$, $p_b = \frac{1-\sqrt{(dc-1)/(d-1)}}{d}$, and $c = \frac{1}{|\mathbf{P}|}I(\mathbf{P}|\rho)$ is the average index of coincidence.

This inequality is a direct result of the fact that the right-hand side of (22) is convex with respect to c. When $\alpha > 2$, Eq. (22) is improved from Rastegin's lower bounds L_{Ras1} [28] and L_{Ras2} [33],

$$\begin{cases} L_{\mathrm{Ras1}} = \dfrac{\alpha}{2(1-\alpha)}\log_2 c, \\ L_{\mathrm{Ras2}} = \dfrac{\alpha-2}{1-\alpha}\log_2\left(\dfrac{1+\sqrt{(dc-1)(d-1)}}{d}\right) \\ \qquad\qquad + \dfrac{1}{1-\alpha}\log_2 c, \end{cases} \tag{23}$$

and when $\alpha = 2$ they all reduce to $-\log_2 c$. A comparison between these results when $\alpha = 3$ and $d = 8$ is shown in Fig. 5.

C. Entropy region

The entropies of performing a finite ordered set of generalized measurements $\mathbf{P} = \{\mathcal{P}^m\}$ on a d-dimensional system described by ρ form a vector, the mth element of which is

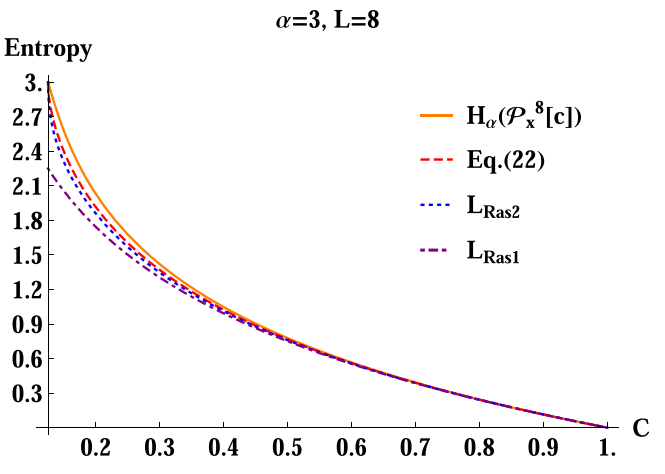

FIG. 5. Lower bound on Rényi 3-entropy of a single probability distribution.

$H(\mathcal{P}^m|\rho)$. The region of all possible entropic vectors induced by $\mathbf{P}$ is called the entropy region of $\mathbf{P}$. The entropy region of a given measurement set contains much more information besides the entropic lower bound, and we expect it to be as meaningful in quantum information theory as in the classical counterpart.

We make a comparison here between the Shannon entropy region for three MUBs in $\mathcal{H}_d$ and that of three probability distributions over d outcomes satisfying

$$\frac{3}{d} \leqslant \sum_{m=1}^{3} I(\mathscr{P}^m) \leqslant \max_{\rho}\{I(\mathbf{B}|\rho)\} = 1 + \frac{2}{d}. \qquad (24)$$

As can be seen in Fig. 6, the entropy region of probability distributions satisfying Eq. (24) is the same as that for three MUBs when $d = 2$, while in higher dimensions distinctions show up at places where the sum of entropies is relatively small, which is in accordance with the information diagrams.

V. DISCUSSIONS

We can see from Figs. 3, 4, and 7 that the tight lower Rényi entropic ($\alpha < 2$) bound curves for both complete MUBs and SIC-POVMs are nondifferentiable at $\mathrm{Tr}(\rho^2) = \frac{1}{k}$ ($\forall k = 2, \ldots, d-1$), which divide the curves into $d-1$ sections. A natural thought is that different sections correspond with density matrices at different boundaries of the set of positive semidefinite Hermitian matrices, namely, different sections of the lower bound curve are attained by density matrices of different ranks.

Conjecture. The tight lower bound on Shannon entropy for complete MUBs or SIC-POVMs on $\mathcal{H}_d$ can only be achieved by density matrices satisfying $(\lambda_1, \lambda_2, \ldots) = \mathscr{P}_y^d[\mathrm{Tr}(\rho^2)]$, where $\{\lambda_i\}$ are nonzero eigenvalues of ρ and arranged in descending order.

We believe this conjecture, if confirmed, will be helpful in searching for tight state-independent EURs for complete MUBs and SIC-POVMs, which could be more efficient in applications of quantum information theory.

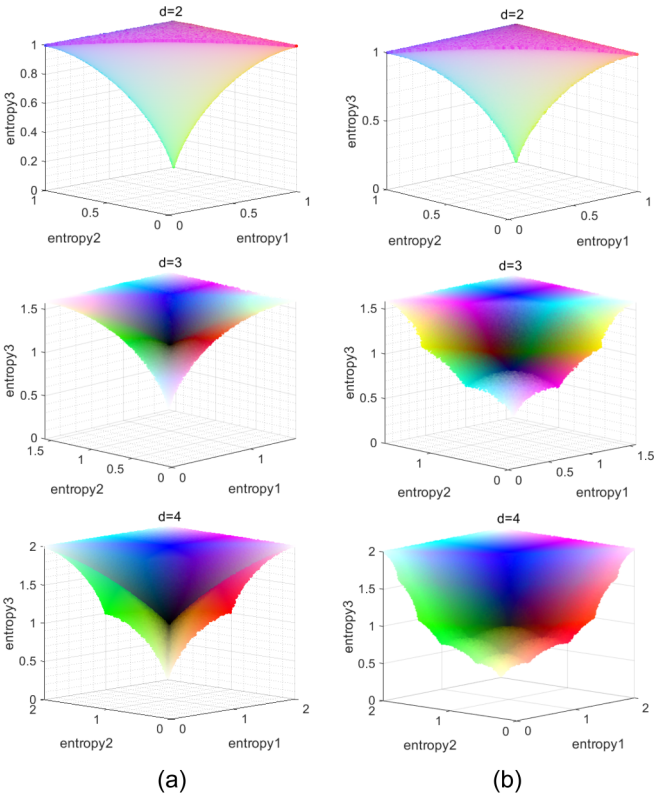

FIG. 6. Shannon entropy regions for three MUBs.

Based on the conjecture above, we have an alternative form of Eq. (16) for MUBs when $\mathrm{Tr}(\rho^2) \leqslant \frac{1}{d-1}$,

$$H(\mathbf{B}|\rho) \geqslant (|\mathbf{B}| - 1)\log_2 d - \mathrm{Tr}[\rho \log_2 \rho], \qquad (25)$$

which coincides with the uncertainty relation for two observables proposed by Berta *et al.* [43].

Lastly, we show an application of entropic uncertainty relations in entanglement detection. Let $\rho_{AB} = \sum_i p_i \rho_i^A \otimes \rho_i^B$ be an arbitrary separable state on the bipartite Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$, and $\rho_A = \mathrm{Tr}_B(\rho_{AB})$ and $\rho_B = \mathrm{Tr}_A(\rho_{AB})$ are the reduced density matrices. According to the results shown in Ref. [11], for any nondegenerate observables $\{A_1, A_2, \ldots\}$ on

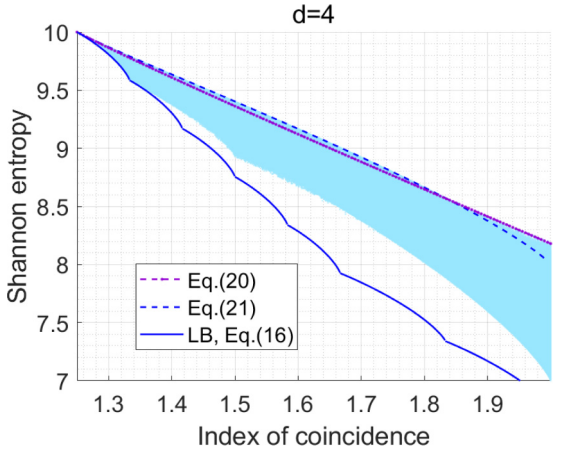

FIG. 7. Information diagram of Shannon entropy for complete MUBs in $\mathcal{H}_4$.

$\mathcal{H}_A$ and $\{B_1, B_2, \dots\}$ on $\mathcal{H}_B$, there is

$$\sum_m H_\alpha(\mathscr{P}(A_m \otimes B_m|\rho_{AB})) \geqslant D = \max\{D_A, D_B\},$$

where

$$D_A = \sum_m H_\alpha(\mathscr{P}(A_m|\rho_A)),$$
$$D_B = \sum_m H_\alpha(\mathscr{P}(B_m|\rho_B)) \quad (\alpha > 0). \tag{26}$$

Here, $\mathscr{P}(A_m \otimes B_m|\rho_{AB})$ is the probability distribution induced by measuring $A_m \otimes B_m$ on ρ_{AB}, and $\mathscr{P}(A_m|\rho_A)$ and $\mathscr{P}(B_m|\rho_B)$ are the two corresponding marginal probability distributions.

Any bipartite state violating Eq. (26) must be entangled. When $\{A_m\}$ and $\{B_m\}$ are complementary observables, D is the sum of entropies for measuring ρ_A or ρ_B in MUBs. According to our uncertainty relations in the previous section, a further lower bound for D can be obtained directly from (22) when $\alpha \geqslant 2$ and from (16) when $\alpha = 1$.

As an example, consider a pair of qudits in a Werner state $\mathcal{W}_{AB} = \frac{1-p}{d^2}\mathbf{1}_{d^2} + p|\psi\rangle\langle\psi|$ $(0 \leqslant p \leqslant 1)$, where $|\psi\rangle = \frac{1}{\sqrt{d}}(|0\rangle \otimes |0\rangle + \cdots + |d-1\rangle \otimes |d-1\rangle)$, and $\{\sigma_m\}$ $(m = 1, 2, \dots, M)$ is a set of complementary observables in $\mathcal{H}_d$. The density matrix of a single qudit is then $\mathcal{W}_A = \mathcal{W}_B = \frac{1}{d}\mathbf{1}_d$, which is independent of p. For simplicity, suppose now d is a prime power and $M = d + 1$, in which case $D = (d + 1)\log_2 d$ is state independent, and moreover, the strongest form of (26) becomes

$$\sum_m^{d+1} H_\infty(\mathscr{P}(\sigma_m \otimes \sigma_m|\mathcal{W}_{AB})) \geqslant (d + 1)\log_2 d, \tag{27}$$

since Rényi α-entropy is a nonincreasing function of α. Numerical results show that (27) can be violated for $p > 0.33$ when $d = 2$ and for $p > 0.46$ when $d = 3$. As the bipartite Werner state is entangled if and only if $p > \frac{1}{d+1}$ [44–47], Eq. (27) is strong enough when $d = 2$ but it is not strong when $d = 3$ and fails to detect all entangled states.

From the above example we know that our EURs can be used to detect entanglement, and stronger separability criteria based on our uncertainty relations are also possible. More works on entropic separability criteria can be found in Refs. [11,15,23].

VI. CONCLUSION

In this paper we have obtained improved entropic uncertainty relations for general symmetric informationally complete positive operator-valued measures and mutually unbiased measurements in terms of Rényi entropy, which are shown to be tight for sufficiently mixed states. By random sampling density matrices and calculating the corresponding entropy for a given set of measurements, comparisons between our entropic bounds and the numerical optimal bounds are made via information diagrams. Our investigation of entropic uncertainty relations could provide some insights for further applications of uncertainty relations in information theory.

ACKNOWLEDGMENTS

This work is supported by the National Key R&D Program of China (Grants No. 2017YFA0303703 and No. 2016YFA0301801) and the National Natural Science Foundation of China (Grant No. 11475084).

APPENDIX A: PROOF OF THEOREM 1

With Lagrangian's multiplier method it is easy to prove that for Rényi α entropy to be local extreme in the set $\{\mathscr{P}|\text{length}(\mathscr{P}) = L, I(\mathscr{P}) = c\}$ at $\mathscr{P}$, the positive probabilities in $\mathscr{P}$ take on at most two different values, say, p_a and p_b. We can parametrize these kinds of probability distributions with three parameters as follows: N, the number of positive probabilities; N_a, the number of probabilities being p_a; c, the index of coincidence. We arrange the positive probabilities in descending order and represent the distribution formally as

$$\mathscr{P}[c, N, N_a] = [N_a \odot p_a, (N - N_a) \odot p_b] \quad (1/N \leqslant c \leqslant 1/N_a), \tag{A1}$$

where $N_a \odot p_a$ is shorthand for N_a probabilities being p_a. Combined with the condition that $N_a p_a + (N - N_a)p_b = 1$ and $I(\mathscr{P}[c, N, N_a]) = c$, we have $p_a = \frac{1+\sqrt{(Nc-1)(N-N_a)/N_a}}{N}$ and $p_b = \frac{1-\sqrt{(Nc-1)N_a/(N-N_a)}}{N}$. We can see that $\mathscr{P}[c_1, N, N_a]$ majorizes $\mathscr{P}[c_2, N, N_a]$ if $c_1 > c_2$, thus $H_\alpha(\mathscr{P}[c, N, N_a])$ is a decreasing function of c. To show Theorem 1, note that given any u, c, $\alpha > 0$, and N $(N_a) \in N^+$, the values of N_a (N), p_a, and p_b, if exist, are all *uniquely* determined by (A2):

$$\begin{cases} 0 \leqslant p_b \leqslant p_a, \quad N \geqslant N_a \geqslant 1, \\ N_a p_a + (N - N_a)p_b = 1, \quad N_a p_a^2 + (N - N_a)p_b^2 = c, \quad N_a p_a^\alpha + (N - N_a)p_b^\alpha = u, \end{cases} \tag{A2}$$

$$H_\alpha\left(\mathscr{P}\left[\frac{1}{N} + s, N, N_a\right]\right) = \log_2 N - \frac{\alpha N s}{2\ln 2} + \frac{\alpha(\alpha-2)N^{\frac{3}{2}}N_a s^{\frac{3}{2}}}{4\ln 2(N - N_a)} + o(s^2) \quad \left(0 < s \ll \frac{1}{N}\right). \tag{A3}$$

Hence $H_\alpha(\mathscr{P}[c, N, N_a])$ is monotonic of both N and N_a, and more concretely, taking the above series expansion of entropy into consideration, we have

$$(2 - \alpha)H_\alpha(\mathscr{P}[c, N, N_{a1}]) \geqslant (2 - \alpha)H_\alpha(\mathscr{P}[c, N, N_{a2}]) \quad \left(N_{a1} < N_{a2}, \frac{1}{N} \leqslant c \leqslant \frac{1}{N_{a2}}\right), \tag{A4}$$

$$(2 - \alpha)H_\alpha(\mathscr{P}[c, N_1, N_a]) \leqslant (2 - \alpha)H_\alpha(\mathscr{P}[c, N_2, N_a]) \quad \left(N_1 < N_2, \frac{1}{N_1} \leqslant c \leqslant \frac{1}{N_a}\right). \tag{A5}$$

We can conclude from (A4) and (A5) that for any distribution $\mathscr{P}$ over L outcomes with $I(\mathscr{P}) = c$ there is

$$(2-\alpha)H_\alpha(\mathscr{P}[c,L,1]) \geqslant (2-\alpha)H_\alpha(\mathscr{P}) \geqslant (2-\alpha)H_\alpha(\mathscr{P}[c,N,N-1]), \tag{A6}$$

where N is an integer such that $\frac{1}{N} \leqslant c < \frac{1}{N-1}$, namely, $N = \lceil \frac{1}{c} \rceil$. This completes the proof of Theorem 1.

APPENDIX B: CONCAVITY AND CONVEXITY

Let us reparametrize $\mathscr{P}[c,N,N_a]$ as $\mathscr{P}^*[c,N,\theta]$, where $\theta = 2\arccos\sqrt{N_a/N}$ and $\theta \in [0,\pi)$. We have

$$\begin{aligned} H_\alpha(\mathscr{P}^*[c,N,\theta]) &= \frac{1}{1-\alpha}\log_2\left[N\cos^2\frac{\theta}{2}\left(\frac{1+\sqrt{Nc-1}\tan\frac{\theta}{2}}{N}\right)^\alpha + N\sin^2\frac{\theta}{2}\left(\frac{1-\sqrt{Nc-1}\cot\frac{\theta}{2}}{N}\right)^\alpha\right] \\ &= \frac{1}{1-\alpha}\log_2 M_\alpha(\mathscr{P}^*[c,N,\theta]), \\ (\alpha-1)\frac{\partial^2}{\partial c^2}H_\alpha(\mathscr{P}^*[c,N,\theta]) &= f(\alpha,z,\theta)\frac{\alpha N^{\alpha+1}\sin\frac{\theta}{2}\cos^3\frac{\theta}{2}}{4\ln 2(Nc-1)^{3/2}M_\alpha^2(\mathscr{P}^*[c,N,\theta])}\left(1+\sqrt{Nc-1}\tan\frac{\theta}{2}\right)^{2\alpha-2}, \end{aligned}$$

where, with $z = \frac{1-\sqrt{Nc-1}\cot\frac{\theta}{2}}{1+\sqrt{Nc-1}\tan\frac{\theta}{2}}$ $(0 < z \leqslant \tan\frac{\theta}{2})$,

$$\begin{aligned} f(\alpha,z,\theta) &= \frac{2\tan^2\frac{\theta}{2}}{1+z\tan^2\frac{\theta}{2}}(z^{\alpha-1}-1)^2 + z^{\alpha-1}\left[-\tan^2\frac{\theta}{2}z^{\alpha-1} + z^{1-\alpha} + (\alpha-1)\left(z\tan^2\frac{\theta}{2}-\frac{1}{z}\right) + (2-\alpha)\left(\tan^2\frac{\theta}{2}-1\right)\right] \\ &\geqslant z^{\alpha-1}\left[-\tan^2\frac{\theta}{2}z^{\alpha-1} + z^{1-\alpha} + (\alpha-1)\left(z\tan^2\frac{\theta}{2}-\frac{1}{z}\right) + (2-\alpha)\left(\tan^2\frac{\theta}{2}-1\right)\right], \end{aligned}$$

when $0 < \alpha < 1$ or $\alpha \geqslant 2$ and $0 < \tan\frac{\theta}{2} \leqslant 1$,

$$f(\alpha,z,\theta) \geqslant z^{\alpha-1}\left[-z^{\alpha-1} + z^{1-\alpha} + (\alpha-1)\left(z-\frac{1}{z}\right)\right] \geqslant 0 \Longrightarrow (\alpha-1)\frac{\partial^2}{\partial c^2}H_\alpha(\mathscr{P}^*[c,N,\theta]) \geqslant 0. \tag{B1}$$

As for Shannon entropy, when $0 < z < \tan\frac{\theta}{2} \leqslant 1$,

$$\frac{\partial^2}{\partial c^2}H(\mathscr{P}^*[c,N,\theta]) = \log_2\left(1+z\tan\frac{\theta}{2}\right) - \log_2\left(1-z\cot\frac{\theta}{2}\right) - \frac{1}{1-z\cot\frac{\theta}{2}} + \frac{1}{1+z\tan\frac{\theta}{2}} \leqslant 0. \tag{B2}$$

(B1) and (B2) imply that when $N_a \in [N/2, N]$, $H_\alpha(\mathscr{P}[c,N,N_a])$ is concave with respect to c when $\alpha \leqslant 1$ and convex with respect to c when $\alpha \geqslant 2$.

APPENDIX C: PROOF OF THEOREM 2

Let $\mathbf{g} = \{\mathscr{P}^g\}$ denote the probability distributions at which $\sum_{m=1}^M H(\mathscr{P}^m)$ is minimum under the restriction

$$\forall 1 \leqslant m \leqslant M, \quad \text{length}(\mathscr{P}^m) = L, \quad \sum_{m=1}^M I(\mathscr{P}^m) = \sum_m c^m = c \quad \left(c \text{ is a constant, } c \in \left[\frac{M}{d}, M\right]\right), \tag{C1}$$

where $\mathscr{P}^g$ is the gth distribution in $\mathbf{g}$. First, according to Theorem 1, (A6), and (B2), we have the following:

Property 1. $\mathscr{P}^g$ must be in the form $\mathscr{P}^g = \mathscr{P}_y^L[c^g]$ for any g.

Property 2. At most one element in $\mathbf{g}$, $\mathscr{P}^k$ say, is not uniform in its nonzero part.

It can be proved that for any $1 \leqslant m < n$ $(n, m \in N^+)$,

$$\begin{cases} 1. \quad H\left(\mathscr{P}_y^L[1/n]\right) + H\left(\mathscr{P}_y^L[1/m+s]\right) > H\left(\mathscr{P}_y^L[1/m]\right) + H\left(\mathscr{P}_y^L[1/n+s]\right), \quad 0 \leqslant s \leqslant 1/n/(n-1), \\ 2. \quad H\left(\mathscr{P}_y^L[1/n-s]\right) + H\left(\mathscr{P}_y^L[1/m]\right) \geqslant H\left(\mathscr{P}_y^L[1/m-s]\right) + H\left(\mathscr{P}_y^L[1/n]\right), \quad 0 \leqslant s \leqslant 1/n/(n+1) \end{cases}. \tag{C2}$$

$$\begin{aligned} \text{Note here:} \quad & I\left(\mathscr{P}_y^L[1/n]\right) + I\left(\mathscr{P}_y^L[1/m+s]\right) = I\left(\mathscr{P}_y^L[1/n+s]\right) + I\left(\mathscr{P}_y^L[1/m]\right), \\ & I\left(\mathscr{P}_y^L[1/n-s]\right) + I\left(\mathscr{P}_y^L[1/m]\right) = I\left(\mathscr{P}_y^L[1/m-s]\right) + I\left(\mathscr{P}_y^L[1/n]\right), \end{aligned}$$

with N_g denoting the number of nonzero probabilities of $\mathscr{P}^g$, a direct result of Properties 1 and 2 and (C2) is the following:

Property 3. (1) $\max_{g,g'} |\{N_g - N_{g'}\}| \leqslant 1$; (2) if $N_k = \min_g\{N_g\}$, then $\forall g, N_g - N_k = 0$.

With Properties 1–3, it is enough to determine $\mathbf{g}$ (Theorem 2). To show the first inequality of (C2) we only need to show $\log_2 N - H(\mathscr{P}_y[1/N+s, N, N-1])$ is an increasing function of N. Under the parametrization introduced in Appendix B we

have

$$\log_2 N - H(\mathscr{P}^*[1/N+s,N,\theta]) = \cos^2\frac{\theta}{2}\left(1+\sqrt{Ns}\tan\frac{\theta}{2}\right)\log_2\left[\cos^2\frac{\theta}{2}\left(1+\sqrt{Ns}\tan\frac{\theta}{2}\right)\right],$$
$$\sin^2\frac{\theta}{2}\left(1-\sqrt{Ns}\cot\frac{\theta}{2}\right)\log_2\left[\sin^2\frac{\theta}{2}\left(1-\sqrt{Ns}\cot\frac{\theta}{2}\right)\right] = h(s,N,\theta). \tag{C3}$$

Let $\theta_y(N) = 2\arctan\frac{1}{\sqrt{N-1}}$, then $\mathscr{P}[c,N,N-1] = \mathscr{P}^*[c,N,\theta_y(N)]$,

$$\frac{\partial}{\partial N}h(s,N,\theta) = \frac{s}{N}\frac{\partial}{\partial s}h(s,N,\theta) > 0, \quad \frac{\partial}{\partial\theta}h(s,N,\theta) < 0, \quad \frac{d\theta_y}{dN} < 0,$$
$$\frac{\partial}{\partial N}h(s,N,\theta_y(N)) = \left[\frac{\partial}{\partial N}h(s,N,\theta) + \frac{\partial}{\partial\theta}h(s,N,\theta)\frac{d\theta_y}{dN}\right]\Big|_{\theta=\theta_y(N)} \geqslant 0. \tag{C4}$$

Hence $h(s,N,\theta_y(N))$ is an increasing function of N, and the second inequality of (C2) can be proved similarly.

It turns out that $\mathbf{g}$ is also the set of probability distributions that descends entropy the fastest locally. Consider $c = \frac{M}{L}$ (this is when probability distributions are all uniform) in the beginning and then let c increase, so according to Properties 1, 2, and (A3) obviously the steepest descent of Shannon entropy is given by

$$\left.\begin{array}{ll}
\left\{(M-1)\odot\mathscr{P}_y^L\left[\frac{1}{L}\right],\mathscr{P}_y^L\left[c-\frac{M-1}{L}\right]\right\}, & \frac{M}{L}\leqslant c\leqslant\frac{M-1}{L}+\frac{1}{L-1}\\
\left\{(M-2)\odot\mathscr{P}_y^L\left[\frac{1}{L}\right],\mathscr{P}_y^L\left[\frac{1}{L-1}\right],\mathscr{P}_y^L\left[c-\frac{M-2}{L}-\frac{1}{L-1}\right]\right\}, & \frac{M-1}{L}+\frac{1}{L-1}\leqslant c\leqslant\frac{M-2}{L}+\frac{2}{L-1}\\
\cdots & \cdots\\
\left\{(M-1)\odot\mathscr{P}_y^L\left[\frac{1}{L-1}\right],\mathscr{P}_y^L\left[c-\frac{M-1}{L-1}\right]\right\}, & \frac{M}{L-1}\leqslant c\leqslant\frac{M-1}{L-1}+\frac{1}{L-2}\\
\cdots & \cdots
\end{array}\right\} = \mathbf{g},$$

where $M\odot\mathscr{P}$ is shorthand for M probability distributions being $\mathscr{P}$.

[1] W. Heisenberg, Z. Phys. **43**, 172 (1927).
[2] H. P. Robertson, Phys. Rev. **34**, 163 (1929).
[3] D. Deutsch, Phys. Rev. Lett. **50**, 631 (1983).
[4] L. Dammeier, R. Schwonnek, and R. F. Werner, New J. Phys. **17**, 093046 (2015).
[5] I. Białynicki-Birula, and Ł. Rudnicki, in *Statistical Complexity*, edited by K. Sen (Springer, Dordrecht, 2011), pp. 1–34.
[6] P. J. Coles, R. Colbeck, L. Yu, and M. Zwolak, Phys. Rev. Lett. **108**, 210405 (2012).
[7] S. Friedland, V. Gheorghiu, and G. Gour, Phys. Rev. Lett. **111**, 230401 (2013).
[8] J. B. M. Uffink and J. Hilgevoord, Found. Phys. **15**, 925 (1985).
[9] G. Vallone, D. G. Marangon, M. Tomasin, and P. Villoresi, Phys. Rev. A **90**, 052327 (2014).
[10] V. Giovannetti, Phys. Rev. A **70**, 012102 (2004).
[11] O. Gühne and M. Lewenstein, Phys. Rev. A **70**, 022316 (2004).
[12] Y. Huang, Phys. Rev. A **82**, 012335 (2010).
[13] R. König, S. Wehner, and J. Wullschleger, IEEE Trans. Inf. Theory **58**, 1962 (2012).
[14] F. Dupuis, O. Fawzi, and S. Wehner, IEEE Trans. Inf. Theory **61**, 1093 (2015).
[15] P. J. Coles, M. Berta, M. Tomamichel, and S. Wehner, Rev. Mod. Phys. **89**, 015002 (2017).
[16] K. Kraus, Phys. Rev. D **35**, 3070 (1987).
[17] H. Maassen and J. B. M. Uffink, Phys. Rev. Lett. **60**, 1103 (1988).
[18] I. D. Ivonovic, J. Phys. A **25**, L363 (1992).
[19] J. Sánchez, Phys. Lett. A **173**, 233 (1993).
[20] J. Sánchez-Ruiz, Phys. Lett. A **201**, 125 (1995).
[21] M. A. Ballester and S. Wehner, Phys. Rev. A **75**, 022319 (2007).
[22] S. Wehner and A. Winter, New J. Phys. **12**, 025009 (2010).
[23] S. Wu, S. Yu, and K. Mølmer, Phys. Rev. A **79**, 022104 (2009).
[24] I. Bengtsson, W. Bruzda, A. Ericsson, J.-Å. Larsson, W. Tadej, and K. Życzkowski, J. Math. Phys. **48**, 052106 (2007).
[25] J. M. Renes, R. Blume-Kohout, A. J. Scott, and C. M. Caves, J. Math. Phys. **45**, 2171 (2004).
[26] A. Kalev and G. Gour, New J. Phys. **16**, 053038 (2014).
[27] G. Gour G and A. Kalev, J. Phys. A: Math. Theor. **47**, 335302 (2014).
[28] A. E. Rastegin, Eur. Phys. J. D **67**, 269 (2013).
[29] A. E. Rastegin, Phys. Scr. **89**, 085101 (2014).
[30] B. Chen and S. Fei, Quantum Inf. Process. **14**, 2227 (2015).
[31] K. Wang, N. Wu, and F. Song, Phys. Rev. A **98**, 032329 (2018).
[32] A. Ketterer and O. Gühne, Phys. Rev. Research **2**, 023130 (2020).
[33] A. E. Rastegin, J. Phys. A: Math. Theor. **53**, 405301 (2020).
[34] A. Rényi, in *Proceedings of the 4th Berkeley Symposium on Mathematical Statistics and Probability*, Vol. 1 (University of California Press, Berkeley, CA, 1961), pp. 547–561.
[35] P. Harremoës and F. Topsøe, IEEE Trans. Inf. Theory **47**, 2944 (2001).
[36] A. J. Scott and M. Grassl, J. Math. Phys. **51**, 042203 (2010).
[37] D. M. Appleby, Opt. Spectrosc. **103**, 416 (2007).
[38] A. Kalev, J. Phys. A: Math. Theor. **47**, 265301 (2014).
[39] I. D. Ivonovic, J. Phys. A **14**, 3241 (1981).
[40] W. K. Wootters and B. D. Fields, Ann. Phys. (NY) **191**, 363 (1989).
[41] A. Klappenecker and M. Rötteler, *Finite Fields and Applications* (Springer, Berlin, 2004), pp. 137–144.

[42] A. O. Pittenger and M. H. Rubin, Linear Algebra Appl. **390**, 255 (2004).
[43] M. Berta, M. Christandl, R. Colbeck, J. M. Renes, and R. Renner, Nat. Phys. **6**, 659 (2010).
[44] A. O. Pittenger and M. H. Rubin, Phys. Rev. A **62**, 032313 (2000).
[45] P. Rungta, W. J. Munro, K. Nemoto, P. Deuar, G. J. Milburn, and C. M. Caves, in *Directions in Quantum Optics*, edited by H. J. Carmichael, R. J. Glauber, and M. O. Scully, Vol. 561 (Springer, Berlin, 2001), pp. 149–164.
[46] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).
[47] A. O. Pittenger and M. H. Rubin, Opt. Commun. **179**, 447 (2000).