,

Optimality of entropic uncertainty relations

Kais Abdelkhalek,[1] René Schwonnek,[1] Hans Maassen,[2] Fabian Furrer,[3] Jörg Duhme,[1] Philippe Raynal,[4, 5] Berthold-Georg Englert,[4, 6, 7] and Reinhard F. Werner[1]
[1]*Institut für Theoretische Physik, Leibniz Universität Hannover, Germany*
[2]*Department of Mathematics, Radboud University, Nijmegen, The Netherlands*
[3]*Department of Physics, University of Tokyo, Japan*
[4]*Centre for Quantum Technologies, National University of Singapore, Singapore*
[5]*University Scholars Programme, National University of Singapore, Singapore*
[6]*Department of Physics, National University of Singapore, Singapore*
[7]*MajuLab, CNRS-UNS-NUS-NTU International Joint Unit, UMI 3654, Singapore*

The entropic uncertainty relation proven by Maassen and Uffink for arbitrary pairs of two observables is known to be non-optimal. Here, we call an uncertainty relation optimal, if the lower bound can be attained for any value of either of the corresponding uncertainties. In this work we establish optimal uncertainty relations by characterising the optimal lower bound in scenarios similar to the Maassen-Uffink type. We disprove a conjecture by Englert *et al.* and generalise various previous results. However, we are still far from a complete understanding and, based on numerical investigation and analytical results in small dimension, we present a number of conjectures.

I. INTRODUCTION

As a characteristic trait, quantum systems possess properties that are incompatible — properties that are equally real but mutually exclusive. In a pair of incompatible properties, if we have precise knowledge about one property, what we know about the other is necessarily imprecise. More generally, we can trade knowledge about one property for knowledge about the other and so know both imperfectly, and quantify the lack of knowledge by a suitable measure of uncertainty. Then, the compromises allowed by nature have their mathematical expressions in the form of *uncertainty relations*, which are inequalities that follow from the formalism of quantum theory.

The study of uncertainty tradeoffs originated in Heisenberg's pioneering work[1] of 1927 and was soon brought into a clear mathematical form by Kennard[2]. Weyl gave another early proof[3]. He was apparently unaware of Heisenberg's paper and gives credit for the idea to Pauli, who seems to have learned it from Heisenberg in a letter prior to the publication of [1]. The modern textbook proof combining the Schwarz inequality with the commutation relations is due to Robertson[4]. In this tradition the "uncertainty of observable X in the state ρ" is identified with the root of the variance of the probability distribution of the outcomes of an X-measurement on particles prepared according to ρ, i.e.,

$$\delta X = \sqrt{\mathrm{tr}\,(\rho X^2) - \mathrm{tr}(\rho X)^2}\,, \tag{1}$$

The key requirement for Heisenberg's uncertainty relation $\delta Q\,\delta P \geq \hbar/2$ to hold is that these variances are evaluated in the same state. The relation is thus a quantitative expression of the observation that there are no dispersion-free states, and is hence of the type "preparation uncertainty relation". This is in contrast to "measurement uncertainty relations" which express the feature of quantum mechanics that some observables may not be measured jointly, which also implies that any measurement of one observable X implies a disturbance of the other in the sense that it cannot be inferred from a measurement on the state after an X-measurement. This aspect, although more prominent in Heisenberg's paper than the preparation side, was made precise only recently[5] (also [6, 7]).

In this paper we are interested in preparation uncertainty relations for quantum systems of finite dimension d. A standard scenario in which this is of interest is the tradeoff between Welcher-Weg information and interference patterns at a multiport interferometer. In this minimalistic instance of wave-particle duality[8] one observable would detect particles on each of the internal paths of the interferometer, thus detecting a particle-like property, whereas the detectors at the end pick up wave-like interference. Uncertainty in this situation expresses the physical fact that if we prepare incoming particles so that they all go along the same path, we loose the interference contrast and, conversely, that large interference contrast is only possible when all paths are "traversed" with roughly equal probability. Another standard context for finite-dimensional uncertainty relations is quantum information theory, particularly quantum key distribution. Large parts of this theory have been developed in finite dimension, and there are many situations in which the incompatibility as expressed by uncertainty relations plays an important role (e.g. in security proofs[9] of cryptographic protocols).

What is common to these motivating instances of finite-dimensional uncertainty is that the outcomes of the respective observables are labelled in a completely arbitrary way. However, a variance depends not only on the abstract outcomes and their probabilities, but also on the real numbers we assign to them. For example, by multiplying all these numbers by the same factor we also multiply δX. Moreover, variance will change if we permute the outcomes, which is as easy to do with beams in optical fibers as with freely re-codable bits of information. Basically motivated by such considerations, Deutsch[10] suggested to use entropies to quantify the (lack of) sharpness of a probability distribution. This led to the famous entropic uncertainty relation established by Maassen and Uffink[11], to which we will refer to as the *MU bound*. It describes the sharpness tradeoff for the outcome distributions p_X^ρ and p_Y^ρ of two observables X, Y in the same state ρ in terms of their Rényi entropies H_α, H_β (see (6)), provided that these parameters satisfy the *duality relation*

$$\frac{1}{\alpha}+\frac{1}{\beta}=2\ . \tag{2}$$

When the observables X and Y are given in terms of their eigenbases $\{x_i\}$ and $\{y_j\}$, so that $p_X^\rho(i)=\langle x_i|\rho|x_i\rangle$ and $p_Y^\rho(j)=\langle y_j|\rho|y_j\rangle$, the MU bound is

$$H_\alpha(p_X^\rho)+H_\beta(p_Y^\rho)\geq -\log\max_{j,k}|\langle y_k|x_j\rangle|^2\,. \tag{3}$$

The bound becomes zero when the two bases share a vector, and maximal (namely $\log d$) if the bases are mutually unbiased, so that all scalar products $\langle y_k|x_j\rangle$ have the same modulus.

An alternative to entropies would again be variances, once one realizes that for defining a variance it is not really necessary to have $\mathbb{R}$-valued random variables. It suffices to have outcomes in a metric space Ω with metric Δ, so that the variance of a probability measure μ on Ω becomes

$$\mathrm{var}(\mu)=\inf_{\eta\in\Omega}\int\mu(d\omega)\ \Delta(\omega,\eta)^2\,. \tag{4}$$

When $\Omega=\{1,\ldots,d\}$ the only permutation invariant metrics are $\Delta(i,j)=c(1-\delta_{ij})$, and we will just fix the constant $c=1$. Then

$$\mathrm{var}(p)=\min_j\sum_i p(i)\,(1-\delta_{ij})^2=1-\max_j p(j)\,. \tag{5}$$

Up to a rescaling this is the so-called min entropy $H_\infty(p) = -\log \max_j p(j)$.

How then should we write an uncertainty relation in this general context? We will see that it is not wise to fix in advance the functional form of the tradeoff relation between $H_\alpha(p_X)$ and $H_\beta(p_Y)$. Instead, the best and most intuitive representation of the tradeoff is the diagram of all pairs $(H_\alpha(p_X), H_\beta(p_Y))$, ranging over all choices of input states ρ. An advantage of this representation is also that it changes in a simple way by a rescaling like the replacement of the variance (5) by H_∞. For qubits ($d = 2$), all measures of sharpness are functions of each other, so all such diagrams are equivalent. Figure 1 is drawn for the Shannon entropy $H = H_1$. Some details of the diagram of *all* pairs of entropies, shown on the left, are clearly not relevant for the uncertainty tradeoff, in which we ask *how small* we can simultaneously make the entropies. For this question it is the lower left corner of the diagram which matters, i.e., the set in the right diagram. It can be described as adding to any pair of entropies the full closed positive (north-east) quadrant above it. It is completely described by its lower left boundary, consisting of those entropy pairs with the property that for no other state one can have one entropy strictly smaller and the other at least as small. We consider the resulting curve as the complete description of the uncertainty tradeoffs between the entropies involved. Characterising this curve is the aim of this paper.

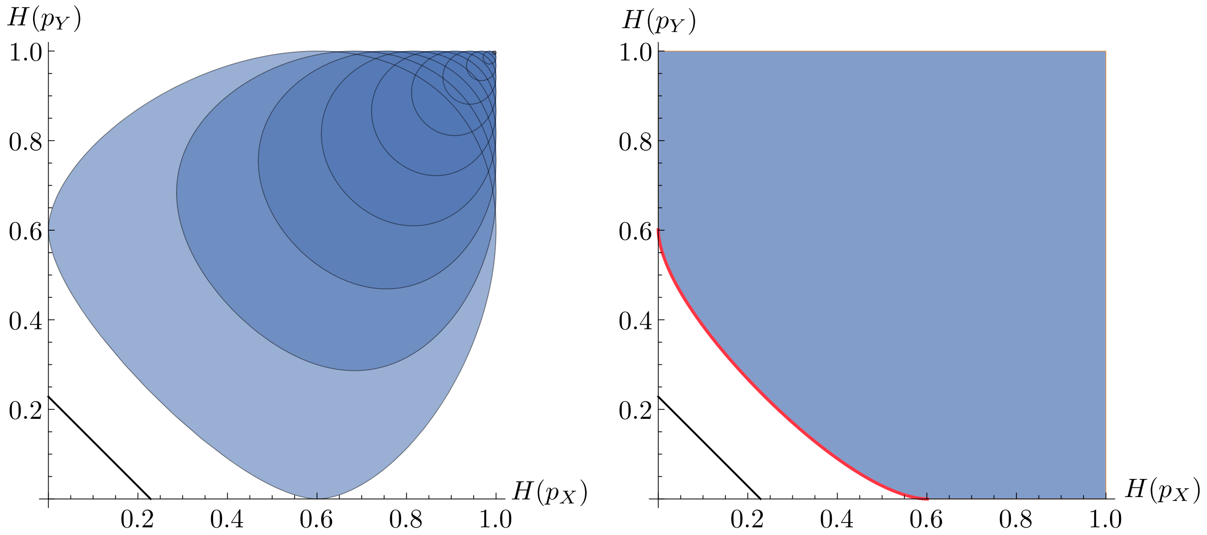

FIG. 1: Entropy pairs for $d = 2$ and the observables $X = \sigma_z$ and $Y = (\sigma_x + \sigma_z)/\sqrt{2}$. Left panel: The shaded set gives all pairs $(H(p_X^\rho), H(p_Y^\rho))$. The contours describe the subsets which can be reached by pure states with a fixed admixture of $\rho = \mathbb{1}/2$. Right panel: The shaded set is the "monotone closure" of the one on the left (see text). The solid curve represents the optimal bound: For entropy pairs on this bound it is impossible to reduce one entropy without enlarging the other. The thin line closer to the origin is the MU bound.

We will always consider a quantum system in a d-dimensional Hilbert space, and consider two projection valued observables with d outcomes. This amounts to the choice of two bases $\{x_i\}$ and $\{y_j\}$, and for the question at hand the choice is completely described by the unitary overlap matrix $U_{ij} = \langle x_i | y_j \rangle$ modulo multiplication by diagonal unitary matrices or permutation matrices from either side. In the motivating standard case, closest to the case of position and momentum of continuous variables, the U represents the discrete Fourier transform of either the cyclic group of n elements or, if n is composite, another finite abelian group of order n. More generally, we also consider complex Hadamard matrices, i.e., unitary operators such that $|U_{ij}| = 1/\sqrt{d}$ for all

i, j. The bases are then called mutually unbiased, and we can think of a multiport interferometer generalizing a 50:50-beam splitter. Such bases also represent complementary pairs of measurements from the informational point of view. However, we will not restrict our study to these special classes of unitary matrices — several results will hold for arbitrary unitary matrices. For generalized observables (POVMs) or k-tuples of observables similar questions can be asked, but we will not consider them in this paper. For the quantification of uncertainty or unsharpness we use the Rényi entropies H_α ($1/2 \leq \alpha \leq \infty$), and denote by $H = H_1$ the standard case of the Shannon entropy. Mostly we assume that the Rényi parameters α and β used for X and Y, respectively, satisfy the duality relation (2). Again, the questions make sense also for other measures, e.g., related to majorization, or for variances, but these will not be considered here. We will also restrict ourselves to state-independent bounds, i.e., to the entropy pairs achievable by arbitrary states. When more is known about the state, for example about further expectation values, the entropy diagram for the subset may be quite different. Thus we do not consider inequalities like the Robertson inequality for variances, where the lower bound depends on the expectation of a commutator.

Outline. In Sect. II we briefly define all the relevant quantities and state our problem in precise mathematical terms. We present a brief review of previous results in Sect. III. In Sect. IV we provide a characterization of the case of equality in the MU bound and thereby show that the MU bound is not optimal in almost all cases. Our main results are presented in Sect. V. We are not able to completely solve the problem in all its generality. However, we provide strong conjectures (Sect. V E) which, if true, heavily reduce the complexity of the problem.

II. PRELIMINARIES AND NOTATION

For $\alpha \in [\frac{1}{2}, \infty]$ the *α-Rényi entropy* of a probability distribution $p \in (0,1)^d$ is defined by

$$H_\alpha(p) = \begin{cases} \frac{1}{1-\alpha} \log \sum_{j=1}^d p(j)^\alpha & \text{if } \alpha \neq 1, \infty \\ -\sum_{j=1}^d p(j) \log p(j) & \text{if } \alpha = 1 \\ -\log \max_j p(j) & \text{if } \alpha = \infty\,. \end{cases} \tag{6}$$

The logarithms can be taken in any base (as long as it is always the same base). We follow the information theory convention of using base-2 logarithms, although base d would also be natural in our context, as it would normalize the range to $0 \leq H_\alpha(p) \leq \log d = 1$. Monotone functions of the entropies tell the same story. In this sense we also cover "Tsallis entropies" $T_\alpha(p) = (1-\alpha)^{-1}(1 - \sum_j p(j)^\alpha)$.

Each entropy diagram will be drawn for a fixed choice of observables (i.e., bases) X, Y and values of the Rényi parameters α, β, so that we consider a map f from the state space to $\mathbb{R}_+^2$ given by

$$f(\rho) = \big(f_1(\rho), f_2(\rho)\big) = \big(H_\alpha(p_X^\rho), H_\beta(p_Y^\rho)\big)\,. \tag{7}$$

For any choice we can define the order relation $\sqsubseteq$ on the state space, so that $\rho \sqsubseteq \rho'$ stands for "$f_1(\rho) \leq f_1(\rho')$ and $f_2(\rho) \leq f_2(\rho')$". The *uncertainty diagram* is the monotone closure of the range $\{f(\rho)\}$, i.e., it is the set S containing precisely the pairs $(h_1, h_2) \in S$ for which there is a state ρ with $f_i(\rho) \leq h_i$ for $i = 1, 2$ (compare FIG. 1). We call a state ρ *optimal* if $\rho' \sqsubseteq \rho$ implies $\rho \sqsubseteq \rho'$, and hence $f(\rho) = f(\rho')$. The corresponding *optimal points* in the entropy plane are characterized by the property that the uncertainty diagram contains no points to their south-west. We call the set of all optimal points the curve of minimal entropies or the *optimal bound*. Therefore the optimal bound corresponds to a function $\gamma : (0, \log d) \to (0, \log d)$ for which

$$H_\alpha(p_X^\rho) \geq \gamma\big(H_\beta(p_Y^\rho)\big) \tag{8}$$

with the property that equality can be obtained for all possible values of $H_\beta(p_Y^\rho)$.

If for some state the MU bound is saturated we call this state an *equality state*. The corresponding point in the entropy plane is an *equality point*. If an equality point exists we call the MU bound *tight*. The MU bound is said to be *optimal*, whenever it completely coincides with the optimal bound.

A Hadamard matrix is a unitary matrix U with elements satisfying $|U_{jk}| = 1/\sqrt{d}$. The Fourier matrix is the matrix U^F with components satisfying

$$U_{jk}^F = \frac{1}{\sqrt{d}}\, \mathrm{e}^{\frac{2\pi \mathrm{i}}{d} jk} \ , \quad j, k = 0, ..., d-1 \ . \tag{9}$$

The Fourier matrix is hence a special instance of a Hadamard matrix. This example generalizes to the wider setting of *finite abelian groups*, rather than just the cyclic group of d elements as in (9). To this end we consider the index set J for the first matrix index of U to equipped with a commutative binary operation "+" turning it into a group. The second index is similarly labelled by the so-called dual group, denoted here by K. A symmetric way to express the relation between these groups is via the canonical bicharacter of the pair (J, K), which is a function $\zeta : J \times K \to \mathbb{C}$. It has the property that the for every k the function $j \mapsto \zeta(j, k)$ is a homomorphism from J to the complex numbers with modulus 1, and that, conversely every such homomorphism is of this form for some unique $k \in K$. Moreover, the same is true vice versa for the functions $k \mapsto \zeta(j, k)$ with fixed $j \in J$. The Fourier matrix in this case is $U_{jk} = d^{-1/2}\zeta(j, k)$, where $d = |J| = |K|$. It is unitary and obviously a Hadamard matrix. When d is not a prime there are several non-isomorphic abelian groups of order d.

III. PREVIOUS RESULTS

There has been considerable work to generalize and improve the MU bound, e.g. by using more general entropy functions [12] or more than two observables [13–16] (see also [17] for a review on entropic uncertainty relations). Most efforts, however, considered only the sum of the entropies (e.g. [18–25]), thereby already fixing the functional form of the tradeoff relation and not capturing all the information contained in the entropy diagram.

In this work we are instead interested in characterising the curve of minimal entropies which we consider the optimal lower bound on the two entropies involved. There are, to the best of our knowledge, only very few results in the literature about the curve of minimal entropies in the finite-dimensional setting. In [26, 27] the authors note that the MU bound is not optimal in the simplest case of dimension $d = 2$ and compute the optimal bound for general unitary operators, but restricted to the Shannon case $\alpha = \beta = 1$. In [8] a conjecture about the entropy minimizing states is presented. We will see that this conjecture needs improvement.

IV. EQUALITY IN THE MAASSEN-UFFINK UNCERTAINTY RELATION

The MU bound provides a lower bound on the sum of two Rényi entropies that satisfy the duality relation (2). When characterising the curve of minimal entropies, it is natural to first investigate the case of equality in the MU bound. If the unitary operator linking the observables is a Hadamard matrix, it is clear that the MU bound is tight. Indeed, any eigenvector of the observables, $\{x_i\}$ or $\{y_i\}$, is an equality state. But can one also find equality points for arbitrary unitary operators?

There already exist some results in the literature discussing this question, most importantly [28] and [29]. In the latter work the authors show the link between the two concepts of uncertainty principle and data processing inequality. Using this link the characterisation of all states that saturate the uncertainty relation reduces to the question of characterising all states for which the application of a certain channel does not imply loss of information. Employing this technique the authors can characterize all quantum states that saturate the MU bound in the restricted setting of observables related by Fourier transformation and Shannon entropies. A more general result was obtained in [28], namely a complete characterisation of all equality points in the special case $\alpha = \beta = 1$, i.e. for Shannon entropies. Here we present an alternative proof of the uncertainty relation which allows us to generalize these from Shannon entropies to the case of arbitrary pairs of Rényi entropies that satisfy the duality relation.

The main result of this section is the following Theorem. In its formulation the "support" of a probability distribution is the set of points with non-zero probability, and $|M|$ denotes the number of elements of a set M.

Theorem IV.1. *Let $\alpha, \beta > \frac{1}{2}$ be such that $1/\alpha + 1/\beta = 2$, and let X, Y be bases with $c = \max_{j,k} |\langle y_k | x_j \rangle|$. Let ρ be a state, and denote by s_X and s_Y the supports of the distributions p_X^ρ and p_Y^ρ. Then equality in the MU uncertainty relation*

$$H_\alpha(p_X^\rho) + H_\beta(p_Y^\rho) \geq \log \frac{1}{c^2} \tag{10}$$

is reached if and only if $\rho = |\psi\rangle\langle\psi|$ is a pure state and, possibly after multiplying the basis vectors x_i, y_j with suitable phases, the following condition holds:

$$\langle x_i|\psi\rangle = |s_X|^{-1/2} \ , \quad \langle y_j|\psi\rangle = |s_Y|^{-1/2}, \quad \text{and} \quad \langle y_j|x_i\rangle = c \quad \text{for } i \in s_X \text{ and } j \in s_Y. \tag{11}$$

Moreover,

$$|s_X|\,|s_Y| = \frac{1}{c^2}. \tag{12}$$

Proof. We assume first that $\rho = |\psi\rangle\langle\psi|$ is pure, and will show that this choice is even necessary at the end of the proof. We fix ψ from now on, and choose phases for the basis elements so that, for $i \in s_X$, $j \in s_Y$ we have

$$\varphi_i = \langle x_i|\psi\rangle > 0 \quad \text{and} \quad \widehat{\varphi}_j = \langle y_j|\psi\rangle > 0. \tag{13}$$

Note that this will change neither c nor the probability distributions. Furthermore, we assume without loss of generality that $\alpha \leq \beta$. We usually eliminate β by the duality relation, so the basic parameter to choose is α with $1/2 < \alpha \leq 1$.

Our proof is inspired by interpolation theory, and involves the application of the maximum principle to a certain analytic "magic function" F. We do not pretend that finding this function is straightforward, since we also came by it in several stages of generalization and simplification. We define

$$F(z) \ = \ c^{1-z}\lambda^z \sum_{i,j\in s} \varphi_i^{\alpha z} \ \langle x_i|y_j\rangle \ \widehat{\varphi}_j^{\beta z} \tag{14}$$

$$\text{with} \quad \lambda \ = \ \left(\|\varphi^\alpha\|_2 \, \|\widehat{\varphi}^\beta\|_2\right)^{-1}, \tag{15}$$

where "$i, j \in s$" is short hand for $i \in s_X$ and $j \in s_Y$, and φ^α is the componentwise power of φ, so that

$$\|\varphi^\alpha\|_2^2 = \sum_i \varphi_i^{2\alpha}, \tag{16}$$

and similarly for $\widehat{\varphi}$. The domain $\mathcal{G}$ on which this function is analyzed is the strip

$$\mathcal{G} = \{z \in \mathbb{C} \,|\, 1 \leq \operatorname{Re} z \leq 2\}, \tag{17}$$

which is also depicted in FIG. 2. Now since the sum (14) is finite and $|r^{\alpha z}| = r^{\alpha \operatorname{Re} z}$ is bounded on $\mathcal{G}$ for every $r > 0$, F is also bounded on $\mathcal{G}$, and the restriction of an entire analytic function. We claim that it is bounded in absolute value by 1. We estimate this separately for the two boundary lines. That is, for $r \in \mathbb{R}$ we have, with $U_{ij} = \langle x_i | y_j \rangle$

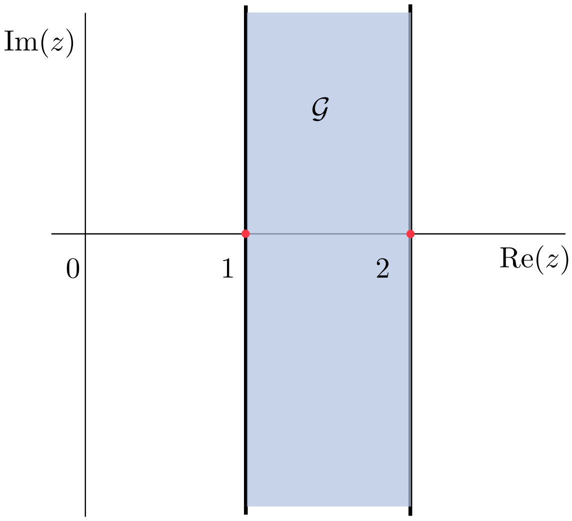

FIG. 2: Domain of F in the complex plane

$$\begin{aligned}
|F(1+\mathrm{i}r)| &= \lambda \left| \sum_{i,j \in s} \varphi_i^{\alpha(1+\mathrm{i}r)} \; U_{ij} \widehat{\varphi}_j^{\beta(1+\mathrm{i}r)} \right| \\
&= \lambda \left| \langle \varphi^{\alpha(1-\mathrm{i}r)} | U | \widehat{\varphi}^{\beta(1+\mathrm{i}r)} \rangle \right| \\
&\leq \lambda \|\varphi^{\alpha(1-\mathrm{i}r)}\|_2 \|\widehat{\varphi}^{\beta(1+\mathrm{i}r)}\|_2 \\
&= \lambda \|\varphi^\alpha\|_2 \, \|\widehat{\varphi}^\beta\|_2 = 1. \qquad (18)
\end{aligned}$$

On the other hand,

$$\begin{aligned}
|F(2+\mathrm{i}r)| &= c^{-1}\lambda^2 \left| \sum_{i,j \in s} \varphi_i^{\alpha(2+\mathrm{i}r)} \; U_{ij} \widehat{\varphi}_j^{\beta(2+\mathrm{i}r)} \right| \\
&\leq \lambda^2 \sum_{i,j \in s} \varphi_i^2 \; |U_{ij}/c| \; \widehat{\varphi}_j^{2\beta} \qquad (19) \\
&\leq \lambda^2 \sum_{i,j \in s} \varphi_i^{2\alpha} \; \widehat{\varphi}_j^{2\beta} \qquad (20) \\
&= \lambda^2 \|\varphi^\alpha\|_2^2 \, \|\widehat{\varphi}^\beta\|_2^2 = 1. \qquad (21)
\end{aligned}$$

Hence, by the maximum principle, $|F(z)| \leq 1$ for all $z \in \mathcal{G}$.

In order to relate this to entropies we consider the special value $z = 1/\alpha$, which always lies in the strip, but for $\alpha = 1$ is a boundary point. We get

$$\begin{aligned}
F\left(\frac{1}{\alpha}\right) &= c^{1-1/\alpha}\lambda^{1/\alpha} \sum_{ij \in s} \varphi_i \; U_{ij} \widehat{\varphi}_j^{\beta/\alpha} \\
&= c^{1-1/\alpha}\lambda^{1/\alpha} \sum_j \widehat{\varphi}_j^{1+\beta/\alpha} \qquad (22) \\
&= c^{1-1/\alpha} \big(\|\varphi^\alpha\|_2^{-1/\alpha} \, \|\widehat{\varphi}^\beta\|_2^{-1/\alpha} \big) \|\widehat{\varphi}^\beta\|_2^2 \qquad (23) \\
&= c^{1-1/\alpha} \|\varphi^\alpha\|_2^{-1/\alpha} \, \|\widehat{\varphi}^\beta\|_2^{1/\beta}, \qquad (24)
\end{aligned}$$

where at (22) we used that $\sum_i \varphi_i U_{ij} = \widehat{\varphi}_j$, and at (23) the definition of λ and duality of α and β. For taking the logarithm of this expression we use that

$$\begin{aligned} \log\bigl(\|\varphi^\alpha\|_2^{-1/\alpha}\bigr) &= -\frac{1-\alpha}{2\alpha} H_\alpha(\varphi^2) \\ \text{and} \quad \log\bigl(\|\widehat{\varphi}^\beta\|_2^{1/\beta}\bigr) &= \frac{1-\beta}{2\beta} H_\beta(\widehat{\varphi}^2) = H_\beta(\widehat{\varphi}^2) \end{aligned} \tag{25}$$

and get, equivalently to $F(1/\alpha) \leq 1$, the inequality

$$\log F\left(\frac{1}{\alpha}\right) = -\frac{1-\alpha}{2\alpha}\Bigl(\log(c^2) + H_\alpha(\varphi^2) + H_\beta(\widehat{\varphi}^2)\Bigr) \leq 0. \tag{26}$$

For $\alpha \neq 1$ we cancel the common factor and get the MU inequality. For $\alpha = 1$ we always get $F(1) = 1$, and the MU inequality is obtained by taking the limit $\alpha \to 1$. However, it is better to express it instead by the derivative of F. For $\alpha = \beta = 1$ we get

$$F'(1) = -\log c - \frac{1}{2} H_1(\varphi^2) - \frac{1}{2} H_1(\widehat{\varphi}^2) \leq 0, \tag{27}$$

because for small ε we must have $F(1+\varepsilon) \leq 1$.

The advantage of this derivation of the MU inequality is that we have powerful characterizations of the equality case. So suppose that equality holds in the MU inequality. Then for $\alpha < 1$ this means that F attains its maximum modulus 1 at the interior point $1/\alpha$ of the strip $\mathcal{G}$, and the Phragmén-Lindelöf Theorem[30] tells us that $F = 1$ is the constant function. For $\alpha = 1$ we need a variant of the maximum principle due to Hopf[31] (see, e.g. Thm. 2.7 in [32]), saying precisely that if the maximum is attained at the boundary with vanishing derivative we once again must have a constant function. In either case we conclude that $F(z) = 1$ for all $z \in \mathcal{G}$.

With this information we can go back to the above estimates for (21), which must now be tight. The first step, the triangle inequality (19), is tight if all terms in the sum have the same argument, so up to a common phase the U_{ij} for $i \in s_X$ and $j \in s_Y$ must be positive. With the phase convention (13) this means $U_{ij} > 0$ for all i, j in the supports. The second estimate (20) is only tight when all U_{ij} also have the maximum allowed modulus c. Hence $U_{ij} = c$. If we consider U as an operator on vectors with support s_Y it thus maps to constant functions, so φ must be constant on s_X. By the same token $\widehat{\varphi}$ must be constant on s_Y. Taking into account the normalizations we get all assertions of the theorem in the pure case $\rho = |\psi\rangle\langle\psi|$.

It remains to show that all equality states must be pure. So let ψ now be any unit vector in the support of ρ and $\sigma = |\psi\rangle\langle\psi|$. Then we can write $\rho = \lambda\sigma + (1-\lambda)\rho'$ with $\lambda > 0$, ρ' some other state, and similar convex relationships for the probability distributions. By concavity of the entropies, σ must also be an equality state. Moreover, by strict concavity, σ and ρ must have the same distributions $p_X^\sigma = p_X^\rho$ and $p_Y^\sigma = p_Y^\rho$, and hence the same supports s_X, s_Y. Going through the proof for the pure equality state $|\psi\rangle\langle\psi|$, and in particular adopting the phase conventions made for ψ we find that $U_{ij} = c$ for all $i \in s_X$ and $j \in s_Y$. But then, if we apply U to any other unit vector ψ' in the support of ρ we find that $U\psi'$ is constant on its support s_Y. Hence ψ' equals ψ up to a phase, the support of ρ is one-dimensional, and ρ must be pure.

An alternative proof of the necessity of purity, at least for the Shannon case $\alpha = \beta = 1$, is via inequality[12]

$$H(p_X^\rho) + H(p_Y^\rho) \geq \log\frac{1}{c^2} + H(\rho). \tag{28}$$

Clearly, for equality states the correction term, the von Neumann entropy $H(\rho)$, has to vanish, i.e., the state must be pure. □

An immediate consequence of Theorem IV.1 is that for most overlap matrices no equality states exist, because $1/c^2$ is not an integer. Since the rows of a unitary matrix must be normalized, this integer is at most d, in which case we must have a Hadamard matrix. When $1/c^2 < d$ one can build examples with equality by first solving a unitary matrix completion problem, starting from the known $s_x \times s_Y$ block. One then has to modify the matrix by unitary rotations on the complementary blocks so that all matrix elements become $\leq c$. The lowest-dimensional example is $2 = 1/c^2 < d = 3$, and the overlap matrix

$$U = \begin{bmatrix} a & a & 0 \\ b & -b & a \\ -b & b & a \end{bmatrix} \quad \text{with} \quad a = \frac{1}{\sqrt{2}} \quad \text{and} \quad b = \frac{1}{2}. \tag{29}$$

Some higher-dimensional examples can be generated by replacing the matrix elements a and b by aU_1 and bU_2, where U_1, U_2 are any Hadamard matrices of the same dimension.

By definition, Hadamard matrices have d orthogonal equality states with supports $(|s_X|, |s_Y|) = (1, d)$ and $(d, 1)$, respectively. In prime dimension this is clearly the only possibility. However, even if the dimension is composite there may be no more than this, as the example[33]

$$C_6 = \frac{1}{\sqrt{6}} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & -\eta & -\eta^2 & \eta^2 & \eta \\ 1 & -\eta^{-1} & 1 & \eta^2 & -\eta^3 & \eta^2 \\ 1 & -\eta^{-2} & \eta^{-2} & -1 & \eta^2 & -\eta^2 \\ 1 & \eta^{-2} & -\eta^{-3} & \eta^{-2} & 1 & -\eta \\ 1 & \eta^{-1} & \eta^{-2} & -\eta^{-2} & -\eta^{-1} & -1 \end{bmatrix} \tag{30}$$

with $\eta = \frac{1-\sqrt{3}}{2} + \mathrm{i}\sqrt{\frac{\sqrt{3}}{2}}$, shows. Here one can mechanically check that none of the 300 3×2-submatrices has the property that all elements become equal after multiplication of rows and columns with suitable phases. Hence from Theorem IV.1 it is clear that the point $(\log 3, \log 2)$ on the MU-line is not accessible for any state.

In the special case of a Fourier matrix (see the end of Sect. II for notations) we can get a complete description of the equality cases from Theorem IV.1, as has been observed in Theorem 4.(1) of [29] for the special case of a cyclic group. We will do the same for an arbitrary finite abelian group J. It turns out that the equality states are then directly linked to the subgroups of J and its dual K. The subgroups always come in pairs, i.e., when $L \subset J$ is a subgroup, so is its annihilator[34]

$$L^\perp = \{k \in K \,|\, \forall j \in L \; \zeta(j,k) = 1\} \subset K. \tag{31}$$

The basic result about annihilators is that $(L^\perp)^\perp = L$ for every subgroup, so there is a ono-to-one correspondence between the subgroups of J and K, under which $L_1 \subset L_2 \Leftrightarrow L_1^\perp \supset L_2^\perp$. For any non-empty set $L \subset J$, we denote by χ_L the ℓ^2-normalized indicator function, i.e., $\chi_L(j) = |L|^{-1/2}$ for $j \in L$ and $\chi_L(j) = 0$ otherwise.

Corollary IV.2. *Let J be a finite abelian group, with Fourier matrix U, and $L \subset J$ a subgroup. Then*

$$U\chi_L = \chi_{L^\perp}, \tag{32}$$

and the vectors of the form $\chi'(j') = \zeta(j', k)\, \chi_L(j' - j)$, where $j \in J/L$ and $k \in K/L^\perp$ are an orthonormal basis so that each $|\chi'\rangle\langle\chi'|$ is an equality state. Moreover, all equality states are of this form.

Note that in the formula for χ' we can take arbitrary $j \in J$ and $k \in K$, but two such choices (j_1, k_1) and (j_2, k_2) define the same function χ' when $j_1 - j_2 \in L$ and $k_1 - k_2 \in L^\perp$. This observation is expressed by taking j, k in the respective quotients.

We remark that, by the fundamental structure theorem of finite abelian groups, every such group is a cartesian product of cyclic groups, and has subgroups of every order which divides d (see Thm. 4.3 in [35]). Hence the equality points on the MU line are *all* points $(\log d_1, \log d_2)$ with $d_1 d_2 = d$.

Proof. Let $|\psi\rangle\langle\psi|$ be an equality state. The Theorem then says that for $j \in s_X$, and $k \in s_Y$ we must have $\zeta(j,k) = \mu(k)\nu(j)$ for suitable phase-valued functions $\mu : s_Y \to \mathbb{C}$ and $\nu : s_X \to \mathbb{C}$. Now we can apply translations as in the construction of χ' in the Corollary to get an equality state with $0 \in s_X$ and $0 \in s_Y$, from which we get $\mu(k)\nu(0) = 1$ and $\mu(0)\nu(j) = 1$, so that the functions μ, ν are actually constant. After applying an overall phase factor we can assume without loss of generality, that $\zeta(j,k) = 1$ for $j \in s_X$, and $k \in s_Y$, and that $\psi = \chi_{s_X}$. In terms of annihilators this is expressed equivalently by $s_Y \subset s_X^\perp$ or $s_X \subset s_Y^\perp$.

When $k \in s_X^\perp$ we still have $\zeta(j,k) = 1$ for $j \in s_X$. But then $(U\psi)(k) = (U\psi)(0) > 0$ and we must also have $k \in s_Y$. It follows that $s_X^\perp \subset s_Y$. Combined with the already established reverse inclusion we get that $s_Y = s_X^\perp$ and, symmetrically $s_X = s_Y^\perp$. Note that since any set of the form $A^\perp$ is automatically a subgroup, we have shown that we can take $s_X = L$, $s_Y = L^\perp$ for some subgroup $L \subset J$.

We have so far only shown that $U\chi_L$ is constant on $L^\perp$, namely equal to $\sqrt{|L|/|J|}$, coming from the summation of $|L|$ terms equal to $|L|^{-1/2}$, and observing the overall normalization factor $|L|^{-1/2}$

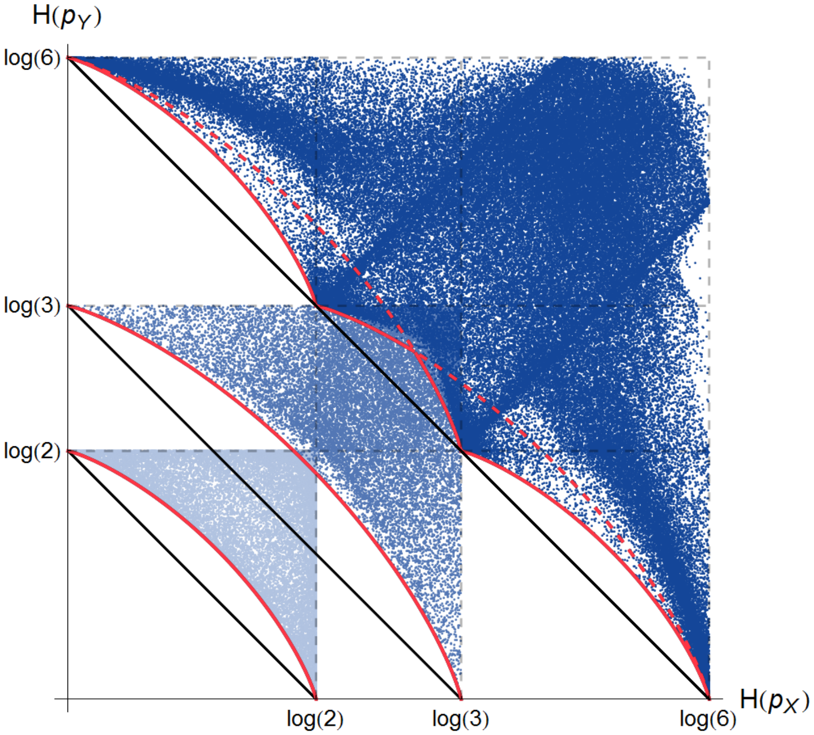

FIG. 3: Numerical sampling of the entropy diagram for dimensions $d = 2$ (light shading), $d = 3$ (medium shading) and $d = 6$ (dark shading) for Fourier-related observables and Shannon entropies. By Theorem IV.1 the number of equality states corresponds to the number of divisors of the respective dimension. The optimal bounds (solid curves) are obtained by applying Conjecture V.6 and Conjecture V.7 presented in Sect. V E.

of the Fourier matrix. We also have to show that $\sum_{j\in L}\zeta(j,k)=0$ whenever $k\notin L^\perp$. However, in that case k induces a non-constant complex homomorphism on L, so it suffices to show that such functions add up to 0 on any finite abelian group. However, this is immediately obvious for cyclic groups, and hence follows for arbitrary groups by the structure theorem. So we conclude that $U\chi_L$ is proportional to $\chi_{L^\perp}$, and since U is unitary, it must be equal, and $|L^\perp|\,|L|=|J|$.

Finally, let us count the translates χ' for a given subgroup. Clearly, they are orthogonal to χ_L whenever either $j+L\cap L=\emptyset$ or $k+L^\perp\cap L\perp=\emptyset$. In other words, by taking one representative g from each class in G/H and also one k from each class in $K/L^\perp$ we get an orthogonal family. This has $(|J|/|L|)\,(|K|/|L^\perp|)=|J|$, i.e., is an orthonormal basis. □

For a product of abelian groups the Fourier matrix is the tensor product of the Fourier matrices of the factors. Moreover one gets many equality states by tensoring, i.e., by taking subgroups of the form $L_1\times L_2\subset J_1\times J_2$. This additive structure is quite apparent from FIG. 3). It is therefore useful to note that this is also true without assuming the group structure. This is shown by the following result.

Corollary IV.3. *Let U_1,U_2 be unitary operators of dimension d_1 and d_2, respectively. Suppose that for each unitary operator there exist an equality state $\sigma^1_{\rm eq}$ and $\sigma^2_{\rm eq}$ as characterized by Theorem IV.1. Then the state $\sigma_{\rm eq}=\sigma^1_{\rm eq}\otimes\sigma^2_{\rm eq}$ is an equality state for the unitary operator $U_1\otimes U_2$.*

Proof. First, note that $\max_{j,k}|(U_1\otimes U_2)_{jk}|=\max_{j,k}|U_{1,jk}|\,\max_{j,k}|U_{2,jk}|$. The MU relation then implies that, for any state σ on a $d_1\,d_2$-dimensional Hilbert space,

$$H_\alpha(p^\sigma_X)+H_\beta(p^\sigma_Y)\geq -2\log\max_{j,k}|(U_1\otimes U_2)_{jk}|=-2\log\max_{j,k}|U_{1,jk}|\,\max_{j,k}|U_{2,jk}|\,. \tag{33}$$

In particular, for the state $\sigma_{\rm eq}=\sigma^1_{\rm eq}\otimes\sigma^2_{\rm eq}$, we have

$$\begin{aligned}H_\alpha(p^{\sigma_{\rm eq}}_X)+H_\beta(p^{\sigma_{\rm eq}}_Y)&=H_\alpha(p^{\sigma^1_{\rm eq}}_X)+H_\alpha(p^{\sigma^2_{\rm eq}}_X)+H_\beta(p^{\sigma^1_{\rm eq}}_Y)+H_\beta(p^{\sigma^2_{\rm eq}}_Y)\\&=-2\log\max_{j,k}|U_{1,jk}|\,\max_{j,k}|U_{2,jk}|\,.\end{aligned} \tag{34}$$

Hence, $\sigma_{\rm eq}$ is an equality state for $U_1\otimes U_2$. □

This Corollary should not be taken to suggest that *only* products will be equality states. For example, take the Fourier matrix of any abelian group of the form $J\times J$, which is the tensor product of two copies of the Fourier matrix of J. Then each subgroup L with $|J|$ elements generates a basis of equality states for the point $(\log|J|,\log|J|)$. These are tensor product states for the subgroup $L=\{(j,0)|j\in J\}=J\times\{0\}$. But for $H=\{(j,j)|j\in J\}$ we get a maximally entangled equality state. Again, the basic idea of this example generalizes to more general settings. If U_1 is any Hadamard matrix and $\overline{U_1}$ its complex conjugate, the maximally entangled vector $\psi=d^{-1/2}\sum_j|jj\rangle$ is invariant under $U=U_1\otimes\overline{U_1}$. Hence both ψ and $U\psi=\psi$ belong to the equidistribution on d points, and $|\psi\rangle\langle\psi|$ is an equality state with entropies $(\log d,\log d)$, just like $|\phi\rangle\langle\phi|$ with $\phi=d^{-1/2}\sum_j|1j\rangle$.

Perhaps one of the more surprising aspects of Theorem IV.1 is that neither the characterization of the equality states nor indeed the value of the lower bound depends on α,β. Hence we have

Corollary IV.4. *Let $\sigma_{\rm eq}$ be an equality state, i.e. it saturates the uncertainty relation for some $\alpha,\beta>\frac{1}{2}$ satisfying the duality relation. Then $\sigma_{\rm eq}$ is also an equality state for all other pairs (α,β) that satisfy the duality relation, including $(\alpha,\beta)=(1/2,\infty),\ (\infty,1/2)$.*

The boundary cases for the inequality are proved by taking the limits on (α,β), and since the lower bound is independent of these, equality carries over. However, additional states may then also

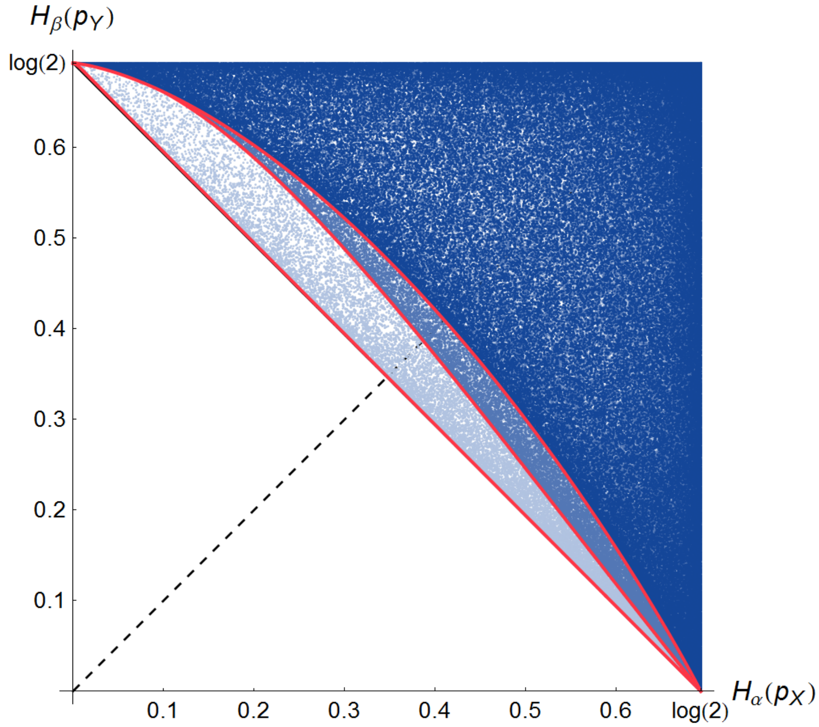

FIG. 4: Typical entropy diagram for Hadamard related observables in prime dimension for different values of α, β satisfying the duality relation (2): $\alpha = 1/2$ (light shading), $\alpha = 0.6$ (medium shading) and $\alpha = 0.75$ (dark shading). The MU bound is optimal if and only if $\alpha = 1/2$.

satisfy equality. Indeed, Theorem IV.1 does not hold in this case. As a counterexample consider an arbitrary Hadamard matrix U. Without loss of generality we can take it dephased, i.e., with all entries in the first row and column equal to $1/\sqrt{d}$. Consider then some arbitrary state $\psi \in \mathbb{R}_+^d$ with real and positive components to find

$$\max_k |(U\psi)_k|^2 \geq |(\tilde{U}\psi)_1|^2 = \frac{1}{d}\left(\sum_k \psi_k\right)^2 . \tag{35}$$

Taking the logarithm and using the definitions (6) this is equivalent to

$$\log d \geq H_{\frac{1}{2}}(p_X^\psi) + H_\infty(p_Y^\psi), \tag{36}$$

which is $\geq \log d$ by the MU inequality. Hence all such states are equality states, and we can continuously interpolate between $H_{\frac{1}{2}} = 0$ and $H_{\frac{1}{2}} = \log d$. Thus the MU bound coincides with the optimal bound (see FIG. 4) and there is a continuum of equality states in contrast to Theorem IV.1.

Another feature is true only in the boundary case, namely that for *every* U there is an equality state. To see this, let us consider an eigenstate x_j of X, for which $H_{1/2}(p_X^{x_j}) = 0$. But at the same time we have

$$\min_j H_\infty(p_Y^{x_j}) = \min_j(-\log \max_k |\langle y_k|x_j\rangle|^2) = -2\log c\ . \tag{37}$$

One could summarize this by saying that in the boundary case $\{\alpha, \beta\} = \{1/2, \infty\}$ the MU bound is just too good to allow a useful characterization of equality.

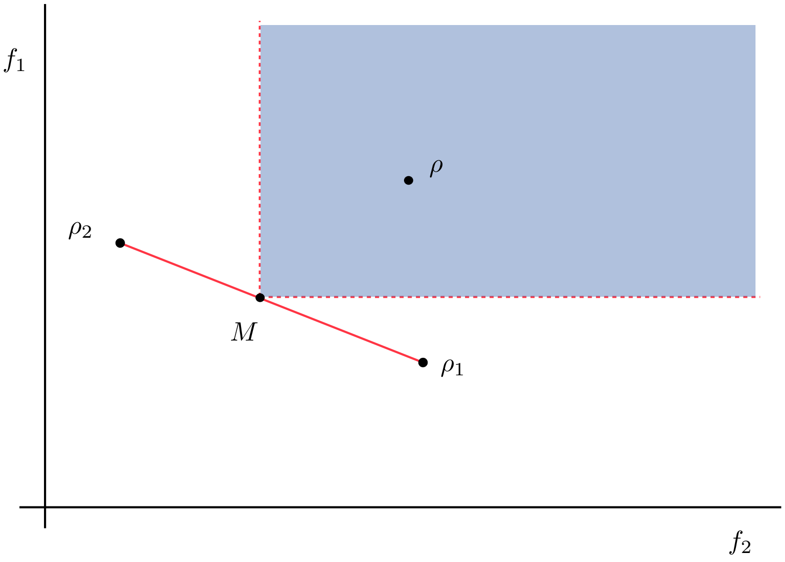

FIG. 5: Consequences of concavity for the set of entropy pairs.

V. CHARACTERISATION OF THE CURVE OF MINIMAL ENTROPY PAIRS

Due to the study of equality in the previous section it is clear that the MU bound is, in almost all cases, not optimal, i.e. it does not coincide with the curve of minimal entropy pairs. To characterize this optimal bound is the aim of this section. We establish three general results that hold for arbitrary dimension: First, we prove that the curve of minimal entropies can be parametrized by pure states. Second, we show that for all real-valued unitary operators we can restrict the problem to real states. And last, we establish a necessary criterion for the Fourier case which all optimal states must satisfy thereby being able to characterize a whole class of potentially optimal states. Additionally, we provide a complete characterisation of the optimal bound for the simplest case of two-dimensional state space, $d = 2$. For $d = 3$ there is an analytic expression[8], which is well-confirmed by numerics, although not proved. However, for higher dimensions the optimal bound remains unknown. Nevertheless, we present random samples that suggest a number of conjectures, which, if true, vastly simplify the characterisation of the optimal bound.

A. Sufficiency of pure states

In this section we show that the optimal bound can be parametrized by pure states. At a first glance, this result may seem not too surprising since the situation is clear when minimizing only one concave functional $f(\rho)$ over all states: In this case one can immediately restrict to pure states, since one of the convex components ρ' of ρ must always give a value $f(\rho') \leq f(\rho)$. However, the situation is not so simple when we consider a pair of concave functions, and the image of the state space under a two-component mapping $f = (f_1, f_2)$ as in (7). The direct consequence of concavity is then that for, say $\rho = (\rho_1 + \rho_2)/2$, the point $f(\rho)$ lies above the midpoint $M = \big(f(\rho_1) + f(\rho_2)\big)/2$ in the coordinatewise ordering, i.e., $f_i(\rho) \geq \big(f_i(\rho_1) + f_i(\rho_2)\big)/2$ for $i = 1, 2$ (see FIG. 5). We therefore cannot conclude that the set $\{f(\rho)\}$ is convex: the midpoint M is not in general in the set. Indeed this is clearly shown by the entropy diagrams, from which it is also clear that the complement is not convex either, except in simple cases.

For the same reasons it is not obvious that it is sufficient to restrict to pure states. This is highlighted by looking at the problem a bit more generally, considering the pairs of probability distributions in two bases.

Proposition V.1. *Consider two orthonormal bases X, Y in a Hilbert space and let p_X^ρ, p_Y^ρ denote the respective probability distributions in the state ρ. Then*

- *If $d = 2$, then for every state ρ there is pure state σ such that $p_X^\rho = p_X^\sigma$ and $p_Y^\rho = p_Y^\sigma$.*
- *If $d \leq 3$, then for every ρ we can find a convex decomposition $\rho = \sum_i \lambda_i \sigma_i$ into pure states σ_i with $p_X^\rho = p_X^{\sigma_i}$ for all i.*

For larger dimensions both statements fail.

Thus, for $d = 2$ the range $\{f(\rho)\}$ is already exhausted by pure states, and for $d = 3$ the monotone closed uncertainty diagram can be computed just with pure states. For if $f(\rho)$ is any point in the diagram, we can decompose into the σ_i, without any increase of f_1, so by concavity we know one of the pure components has smaller f_2. However, this proof strategy will fail for $d \geq 4$.

Proof. (1) For $d = 2$, the set of quantum states ρ with the same distribution p_X^ρ is the intersection of the Bloch ball with a hyperplane. Intersecting with the hyperplane for p_Y^ρ we get a line, which also intersects the Bloch sphere, i.e., there is a pure state with the same distributions.

(not 1) The example uses Fourier transform in $d = 3$. Two density operators have the same position distribution iff their diagonals coincide and the same momentum distribution iff the sums $\sum_x \langle x|\rho|x + y\rangle$ coincide for all y. Now consider a diagonal matrix with diagonal entries $(1, 1, 0)/2$. A pure state with this diagonal will have just one non-zero phase in the 1-2 matrix element, so the sum with $y = 1$ will be non-zero other than for the mixed state.

(2) Let us consider the convex subset $K(p)$ of states with $p_X^\rho = p$. We have to show that for $d = 3$ all extreme points of this set are, in fact, pure. Our method will also show that this fails for $d \geq 4$.

First observe by just conjugating with a positive diagonal operator from right and left we get an isomorphism of $K(p)$ and $K(q)$, as long as p, q have the same support (of size d). So we may as well take p to be uniform, for which we write $K(1)$ (Normalization factors are irrelevant here).

Let us sort the potential extreme points by rank. Full rank is not possible, since then *any* vector with uniform distribution could be subtracted with a positive weight. Rank 1 is uninteresting, because it is of the form we want to exclude. This takes care of $d = 2$ and leaves only the rank 2 case for $d = 3$.

So let us consider the case of rank 2 for general d. Let ϕ_1, ϕ_2 be two linearly independent vectors in the range of the density operator $\rho = |\phi_1\rangle\langle\phi_1| + |\phi_2\rangle\langle\phi_2|$. The condition that ρ has uniform position distribution means that $|\phi_1(x)|^2 + |\phi_1(x)|^2 = 1$ for all x. In other words, the pair $\Phi(x) = \big(\phi_1(x), \phi_2(x)\big) \in \mathbb{C}^2$ is a unit vector for every x . Then we ask whether there is any non-zero vector $\Psi \in \mathbb{C}^d$ of the form $\Psi(x) = \overline{\alpha_1}\phi_1(x) + \overline{\alpha_2}\phi_2(x)$ such that $|\Psi(x)| = 1$ for all x. This would be a convex component of ρ with even distribution, so we could further decompose ρ.

We can read this as a scalar product $|\langle \alpha, \Phi(x)\rangle|^2$. Think of the $\Phi(x)$ and of α as represented on the Bloch sphere, where the geodesic distance is just a function of the above scalar product. So our question reduces to: Given d vectors on the sphere, can we find one further vector which has the same distance from each of them?

Now for $d = 2$ this is obvious, and for $d = 3$ it works just like in the planar geometry of triangles: The locus of all points which have the same distance from $\Phi(1)$ and $\Phi(2)$ is a great circle bisecting their connecting geodesic at a right angle. Intersect with the bisector for $\Phi(2)$ and $\Phi(3)$, which gives a point which has the same distance from all three points. Therefore, for $d = 3$, there are no extreme points of rank 2, hence all are of rank 1 as claimed.

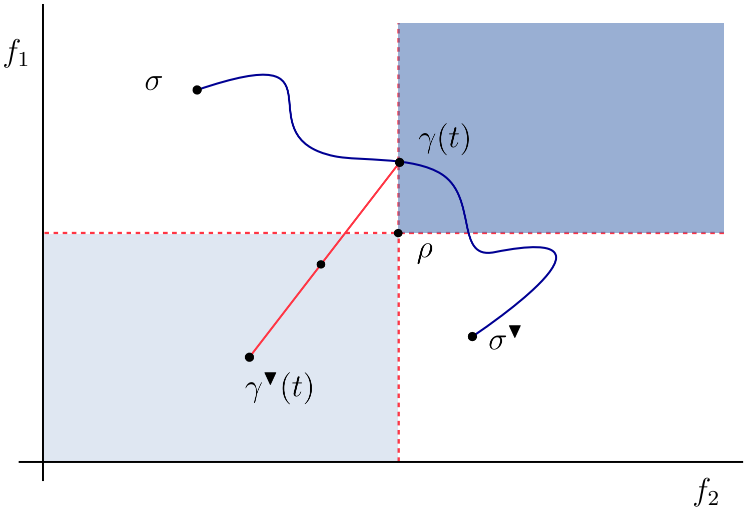

FIG. 6: States appearing in the proof of Theorem V.2 as mapped to the two entropies plane.

For higher d it is easy to find d points, which do not lie on a circle, i.e., there is no point equidistant from all of them. Hence there are extreme points of $K(1)$ of rank 2.

□

Surprisingly however, pure states can be shown to saturate all uncertainty diagrams, practically without assumptions on X, Y, α, β.

Theorem V.2. *Let f_1, f_2 be continuous concave functionals on the state space, define the order relation $\sqsubseteq$ as after equation (7). Then for every state ρ there is a pure state σ such that $\sigma \sqsubseteq \rho$.*

Proof. The plan of the proof is to show that for every non-pure ρ we can find another state σ of strictly smaller rank such that $\sigma \sqsubseteq \rho$. Then we can successively lower the rank, arriving finally at a pure state.

Consider the face F of the state space generated by ρ. Its topological boundary ∂F consists precisely of the possible convex components of ρ of lower rank, and is connected. For each point $\sigma \in \partial F$ there is a unique "antipode" $\sigma^\blacktriangledown$. It is defined as

$$\sigma^\blacktriangledown = \frac{1}{\lambda}\Big(\rho - (1-\lambda)\sigma\Big) \tag{38}$$

for the smallest λ for which the right hand side is positive semidefinite. It is clearly a state of reduced rank, i.e., $\sigma^\blacktriangledown \in \partial F$. We note that the required weight λ cannot be 0 or 1.

We need not consider the case that $\sigma \sqsubseteq \rho$, since otherwise we have found the desired element. Therefore, by exchanging the functions f_1 and f_2 if necessary, we may assume that $f_1(\sigma) > f_1(\rho)$. We cannot also have $f_1(\sigma^\blacktriangledown) \geq f_1(\rho)$. Indeed, this would lead to the contradiction

$$f_1(\rho) \geq (1-\lambda) f_1(\sigma) + \lambda f_1(\sigma^\blacktriangledown) > f_1(\rho). \tag{39}$$

Now consider a continuous curve $[0,1] \ni t \mapsto \gamma(t) \in \partial F$ connecting σ and $\sigma^\blacktriangledown$, i.e., such that $\gamma(0) = \sigma$ and $\gamma(1) = \sigma^\blacktriangledown$ (see FIG. 6). Since f_1 was assumed to be continuous the previous argument shows that, for some t, $f_1\big(\gamma(t)\big) = f_1(\rho)$.

If $f_2\big(\gamma(t)\big) \leq f_2(\rho)$ we have found the desired element $\gamma(t) \sqsubseteq \rho$. The non-trivial case to consider is therefore $f_2\big(\gamma(t)\big) > f_2(\rho)$, or $\rho \sqsubseteq \gamma(t)$. Let $\lambda \in (0,1)$ be the weight so that $\rho =$

$(1-\lambda)\gamma(t)+\lambda\gamma(t)^{\blacktriangledown}$. Then by concavity, for $i=1,2$,

$$\begin{aligned} f_i(\rho) &\geq (1-\lambda)f_i\big(\gamma(t)\big)+\lambda f_i(\gamma(t)^{\blacktriangledown}) \\ &\geq (1-\lambda)f_i(\rho)+\lambda f_i\big(\gamma(t)^{\blacktriangledown}\big) \\ \text{i.e.,}\quad f_i(\rho) &\geq f_i\big(\gamma(t)^{\blacktriangledown}\big). \end{aligned} \tag{40}$$

Therefore $\gamma(t)^{\blacktriangledown} \sqsubseteq \rho$.

□

B. Sufficiency of real states for real unitary matrices

From the previous section we know that for all unitary operators the complete optimal bound can be parametrized by pure states. Now we show that if the unitary matrix linking the two observables is real-valued, then we can further restrict the set of states for the complete optimal bound to the set of real-valued vectors. In this whole subsection we fix the Hilbert space to be $\mathbb{C}^d$ with componentwise complex conjugation, so that the real vectors $\mathbb{R}^d \subset \mathbb{C}^d$ are naturally embedded.

Theorem V.3. *Let f_1, f_2 be continuous concave functionals on the state space and their inputs linked by a real unitary operator U_{real}. Also define the order relation $\sqsubseteq$ as after equation (7). Then for every state ρ there is a pure and real state σ such that $\sigma \sqsubseteq \rho$.*

Proof. The idea of the proof is to employ again the proof technique of Theorem V.2, i.e. decompose a state in two states with the desired property (in this case, real states) and use the concavity property of the functions.

Let $\psi \in \mathbb{C}^d$ be a pure state. Since we are interested in a decomposition into real states, it is natural to consider the decomposition

$$\psi = \sqrt{\lambda}v + \mathrm{i}\sqrt{1-\lambda}w \tag{41}$$

where $v, w \in \mathbb{R}^d$ are the normalized real and imaginary part of ψ and $\lambda = |\operatorname{Re}(\psi)|^2$ ranges from 0 to 1. We are only interested in the case where neither $v \sqsubseteq \psi$ nor $w \sqsubseteq \psi$, otherwise the statement follows immediately. Furthermore, we assume without loss of generality that $f_1(v) > f_1(\psi)$. Similar to the proof in Theorem V.2 we cannot also have that $f_1(w) > f_1(\psi)$ because we would then find the contradiction

$$f_1(\psi) \geq \lambda f_1(v) + (1-\lambda)f_1(w) > f_1(w)\ . \tag{42}$$

Consider now the states

$$\varphi(t) := \mathrm{e}^{\mathrm{i}t}\psi \tag{43}$$

and their normalized real and imaginary part

$$\begin{aligned} \gamma(t) &:= \operatorname{Re}\big(\varphi(t)\big)/|\operatorname{Re}\big(\varphi(t)\big)|\ , \\ \sigma(t) &:= \operatorname{Im}\big(\varphi(t)\big)/|\operatorname{Im}\big(\varphi(t)\big)| \end{aligned} \tag{44}$$

such that

$$\varphi(t) = \sqrt{\mu(t)}\gamma(t) + \mathrm{i}\sqrt{1-\mu(t)}\sigma(t)\ , \tag{45}$$

where $\mu(t) = ||\gamma(t)||$. Note that $f_i(\varphi(t)) = f_i(\psi)$ for all $t \in (0, 2\pi)$. Also note that for a real-valued unitary operator the probability distributions $p_X^{\varphi(t)}$ and $p_Y^{\varphi(t)}$ have the same form

$$p_{X/Y}^{\varphi(t)} = \mu(t) p_{X/Y}^{\gamma(t)} + \big(1 - \mu(t)\big) p_{X/Y}^{\sigma(t)} \ . \tag{46}$$

Due to continuity we know that there exists t_0 such that either $\gamma(t_0) \sqsubseteq \psi$, from which we obtain the desired statement, or $\psi \sqsubseteq \gamma(t_0)$. Using the concavity of the functions f_i, the latter then implies

$$\begin{aligned} f_i(\psi) = f_i\big(\varphi(t_0)\big) &\geq \mu(t_0) f_i\big(\gamma(t_0)\big) + \big(1 - \mu(t_0)\big) f_i\big(\sigma(t_0)\big) \\ &\geq \mu(t_0) f_i(\psi) + \big(1 - \mu(t_0)\big) f_i\big(\sigma(t_0)\big) \ , \end{aligned} \tag{47}$$

from which obtain $f_i\big(\sigma(t_0)\big) \leq f_i(\psi)$, or equivalently $\sigma(t_0) \sqsubseteq \psi$. □

C. Variatonal method

So far we characterized the optimal bound by the order relation $\sqsubseteq$. Equivalently, we may also consider an optimisation problem as mentioned in (8): Given some fixed value of $H_\beta(p_Y^\rho) = \delta$ the optimal bound γ is described by minimising $H_\alpha(p_X^\rho)$, i.e.

$$\gamma(\delta) = \min_\rho \{H_\alpha(p_X^\rho) | H_\beta(p_Y^\rho) = \delta\} \ , \tag{48}$$

where δ ranges from 0 to $\log d$. However, performing this optimisation is in general quite difficult, especially because a nice characterisation of the constant entropy set $\{\rho | H_\beta(p_Y^\rho) = \delta\}$ is not known. Instead, we restrict to optimising over a subset of this constant entropy set, namely states with varied phases. Clearly, this method will not yield a sufficient criterion for a state to be optimal. However, it provides us with a necessary criterion which allows us to identify a whole class of candidates of optimal states.

More concretely, using Theorem V.2 we consider pure states $\varphi \in \mathbb{C}^d$ and denote the components of the phase-varied state in Y basis by

$$\psi_j = \varphi_j \exp\left(\frac{2\pi\mathrm{i}}{d} \theta_j\right) \tag{49}$$

for some phases θ_j. Varying these phases does not change the probability distribution, $p_Y^\psi = p_Y^\varphi$, and hence the phase varied states form a subset of the constant entropy set. For observables linked by Fourier transformation, we can optimize $H_\alpha(p_X^\psi)$ over these states to find the following extremality criterion:

Lemma V.4. *Let the two observables X and Y be linked by the Fourier matrix* (9) *and let ψ denote an optimal state of this setup. Furthermore, let $\hat{\psi}$ denote the Fourier transform of ψ. Then ψ satisfies*

$$\mathrm{Im}\left(\psi_k \sum_{j=1}^d \frac{\partial H_\alpha(p_X^\psi)}{\partial |\hat{\psi}_j|^2} \overline{\hat{\psi}_j} \exp\left(\frac{2\pi\mathrm{i} jk}{d}\right)\right) = 0 \quad \forall k. \tag{50}$$

Proof. In order to optimize $H_\alpha(p_X^\psi)$ we compute

$$\left.\frac{\partial H_\alpha(p_X^\psi)}{\partial \theta_k}\right|_{\theta=0} = \sum_{j=1}^d \frac{\partial H_\alpha(p_X^\varphi)}{\partial |\hat{\psi}_j|^2} \left.\frac{\partial |\hat{\psi}_j|^2}{\partial \theta_k}\right|_{\theta=0} \overset{!}{=} 0 \ . \tag{51}$$

With $\omega := \exp\left(\frac{2\pi \mathrm{i}}{d}\right)$ the Fourier transform of ψ is defined as $\hat{\psi}_j := \frac{1}{\sqrt{d}} \sum_{m=1}^{d} \psi_m \omega^{jm}$ and, hence,

$$|\hat{\psi}_j|^2 = \frac{1}{d} \sum_{m,n=1}^{d} \varphi_m \overline{\varphi_n}\ \omega^{j(m-n)+\theta_m-\theta_n}\ . \tag{52}$$

Therefore we have

$$\begin{aligned} \left.\frac{\partial|\hat{\psi}_j|^2}{\partial\theta_k}\right|_{\theta=0} &= \left.\frac{1}{d} \sum_{m,n=1}^{d} \varphi_m \overline{\varphi_n} \omega^{j(m-n)+\theta_m-\theta_n}\right|_{\theta=0} \\ &= \frac{2\pi \mathrm{i}}{d^2} \operatorname{Im}\left(\varphi_k \overline{\hat{\varphi}_j} \omega^{jk}\right) \end{aligned} \tag{53}$$

Combining (51) and (53) we obtain the desired statement. □

Any optimal state must necessarily satisfy the above criterion. This allows us to characterize a whole class of potentially optimal states:

Lemma V.5. *Let φ be a real-real symmetric state, i.e. a real state, $\varphi \in \mathbb{R}^d$, satisfying the symmetry condition*

$$\varphi(j) = \varphi(d-j) \quad \forall j = 1, ..., d-1 \tag{54}$$

or, equivalently, a real state with real Fourier transform, $\hat{\varphi} \in \mathbb{R}^d$. Then φ satisfies the extremality criterion (50)*.*

Proof. We first note a simple, but important property of real-real symmetric states: If φ is a real-real symmetric state and ξ is a state with components $\xi_j = f(\varphi_j)$, where f is any function taking real numbers to real numbers, then ξ is also a real-real symmetric state. For example, the Fourier transform of any real-real symmetric state is also real-real symmetric.

Now φ is assumed to be real-real symmetric. Hence, $\hat{\varphi}$ is real-real symmetric. Define

$$\xi_j := \frac{\partial H_\alpha(p_X^\psi)}{\partial|\hat{\varphi}_j|^2} \hat{\varphi}_j \tag{55}$$

and note that ξ is also real-real symmetric. Importantly this implies that its Fourier transform, $\hat{\xi}$ is real. We therefore have for all k

$$\operatorname{Im}\left(\varphi_k \sum_{j=1}^{d} \frac{\partial H_\alpha(p_X^\psi)}{\partial|\hat{\varphi}_j|^2} \overline{\hat{\varphi}_j} \exp\left(\frac{2\pi \mathrm{i} jk}{d}\right)\right) = \operatorname{Im}\left(\sum_{j=1}^{d} \xi_j \exp\left(\frac{2\pi \mathrm{i} jk}{d}\right)\right) = \operatorname{Im}\left(\hat{\xi}\right) = 0\ , \tag{56}$$

which finishes the proof. □

D. Simplest case: $d = 2$

The results we presented so far are not sufficient to provide a complete characterisation of the curve of minimal entropy pairs. In what follows we therefore restrict to small dimension in order to reduce the complexity of the problem.

More concretely, we investigate the simplest case, where the dimension of the Hilbert space is $d = 2$. In [26, 27] the authors characterized the curve of minimal entropy pairs for all unitary operators while restricting to the case of Shannon entropies. We now generalize their result to

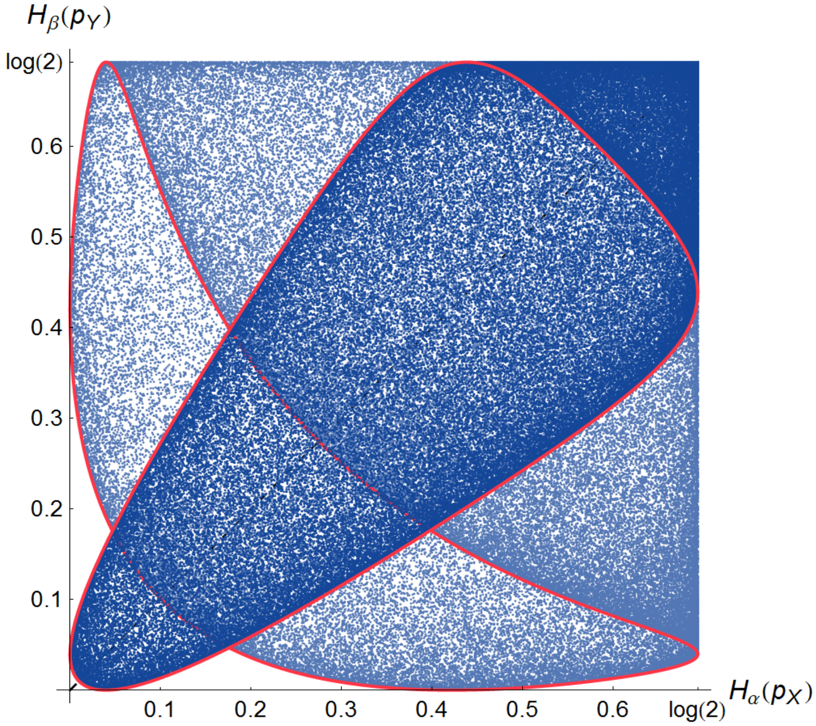

FIG. 7: The optimal bound can be completely characterized in the qubit case (solid curves). The plot illustrates two entropy diagrams for randomly chosen unitary operators and entropy-pairs with $\alpha = \beta = 10$ (light shading) and $\alpha = \beta = 8$ (dark shading).

arbitrary pairs of Rényi entropies: First we show that for each 2×2 unitary operator U there is a real unitary operator $\tilde{U}$ with the same entropy diagram. Then from Theorem V.3 we can immediately infer that the lower bound can be parametrized by real states. More concretely, our aim is to show that any unitary operator, which we can always write in $\{x_i\}$ basis up to an (irrelevant) global phase as

$$U = \begin{pmatrix} \cos(\varphi) & \sin(\varphi)\mathrm{e}^{-\mathrm{i}\theta} \\ -\sin(\varphi)\mathrm{e}^{\mathrm{i}\theta} & \cos(\varphi) \end{pmatrix} , \tag{57}$$

is equivalent to the matrix

$$\tilde{U} = \begin{pmatrix} \cos(\varphi) & \sin(\varphi) \\ -\sin(\varphi) & \cos(\varphi) \end{pmatrix} . \tag{58}$$

Indeed, the entropy diagram does not change if we first modify the unitary operator to $U' = UV$ if V is a unitary operator satisfying $Vx_i = \exp(\mathrm{i}\varphi_i)x_i$ for some phases φ_i and all i, since then for any state ρ there exists a state ρ' that yields the same pair of entropies. To see this, let $\rho' = V^\dagger \rho V$ to find that

$$p_X^{\rho'}(i) = \langle x_i|\rho'|x_i\rangle = \langle x_i|V^\dagger \rho V|x_i\rangle = \langle x_i|\rho|x_i\rangle = p_X^{\rho}(i) \tag{59}$$

and

$$p_{Y'}^{\rho'}(j) = \langle y'_j|\rho'|y'_j\rangle = \langle y_j|VV^\dagger \rho VV^\dagger|y_j\rangle = \langle y_j|\rho|y_j\rangle = p_Y^{\rho}(j) . \tag{60}$$

Now consider the modification

$$U' = \begin{pmatrix} \cos(\varphi) & \sin(\varphi) \\ -\sin(\varphi)\mathrm{e}^{\mathrm{i}\theta} & \cos(\varphi)\mathrm{e}^{\mathrm{i}\theta} \end{pmatrix} \tag{61}$$

obtained via the unitary operator

$$V_\theta = \begin{pmatrix} 1 & 0 \\ 0 & \mathrm{e}^{\mathrm{i}\theta} \end{pmatrix} \tag{62}$$

However, U' yields exactly the same probability distribution as $\tilde{U}$. Hence, by Theorem V.3 the curve of minimal entropy pairs can be parametrized by real states.

Since the real states form a one-parameter family it is not difficult to check that the states

$$\psi = \big(\cos(\xi), \sin(\xi)\big) \ , \tag{63}$$

where the range of ξ is either $(0, \arccos(|U_{1,1}|)$ or $(\arccos(|U_{1,1}|), \pi/2)$ depending on whether $\arccos(|U_{1,1})| \in (\pi/4, 3\pi/4)$ or not, parametrize the curve of minimal entropy pairs for all unitary operators and all Rényi entropies. The problem is therefore completely solved in the simplest case $d = 2$ (see FIG. 7).

E. Numerical sampling and conjectures

In the previous section we characterized the optimal bound in the special case of dimension $d = 2$. To the best of our knowledge the problem is unsolved for all other dimensions. Instead the authors of [8] provide a conjecture stating that the curve of minimal entropies is traced out by states of the form

$$\psi = (\sqrt{p_2}, \sqrt{p_2}, ..., , \sqrt{p_2}, \sqrt{p_1})^{\mathsf{T}} \tag{64}$$

with $p_1 + (d-1)p_2 = 1$ in the case of complex Hadamard matrices and Shannon entropies. Due to the results of [26, 27] it is clear that this conjecture is correct for $d = 2$. The conjecture also holds true in the case $d = 3$ if we trust the numerics presented in FIG. 3, where the solid curve directly corresponds to the states (64). However, for $d = 4$ we show that the conjecture already fails: For complex Hadamard matrices $c = 1/\sqrt{d}$ and, hence, according to our analysis of equality in the MU bound there must be three distinct equality points, whereas the conjectured states only yield two equality points (see FIG. 8).

However, we present two different conjectures which, if correct, explain how the bound in FIG. 3 and 8 can be obtained:

Conjecture V.6. *(Product states for matrices with product form)*
Let the unitary operator U linking the two observables be a matrix of the form $U = U_1 \otimes U_2$. Then for any state ρ there exists a product state $\rho_1 \otimes \rho_2$ with the same pair of entropies.

The consequence of this our first conjecture is that the curve of minimal entropies for product form unitary operators in some composite dimension $d = d_1\, d_2$ is just comprised of tensor products of states that parametrize the curve in dimension d_1 and d_2, respectively. Indeed, from the additivity of the Rényi entropy it then directly follows that a state $\rho_d = \rho_{d_1} \otimes \rho_{d_2}$ is optimal with respect to the unitary operator $U = U_{d_1} \otimes U_{d_2}$ if and only if the marginals ρ_{d_1} and ρ_{d_2} are optimal with respect to the unitary operators U_{d_1} and U_{d_2}, respectively. We note that this conjecture also agrees with our findings for the equality states, especially Corollary IV.3.

Conjecture V.7. *(Decomposition of the Fourier matrix)*
Let the two observables be linked by the Fourier matrix U_d^F of composite dimension $d = d_1\, d_2$. Then the entropy diagram does not change if we replace U_d^F by $U_{d_1}^F \otimes U_{d_2}^F$.

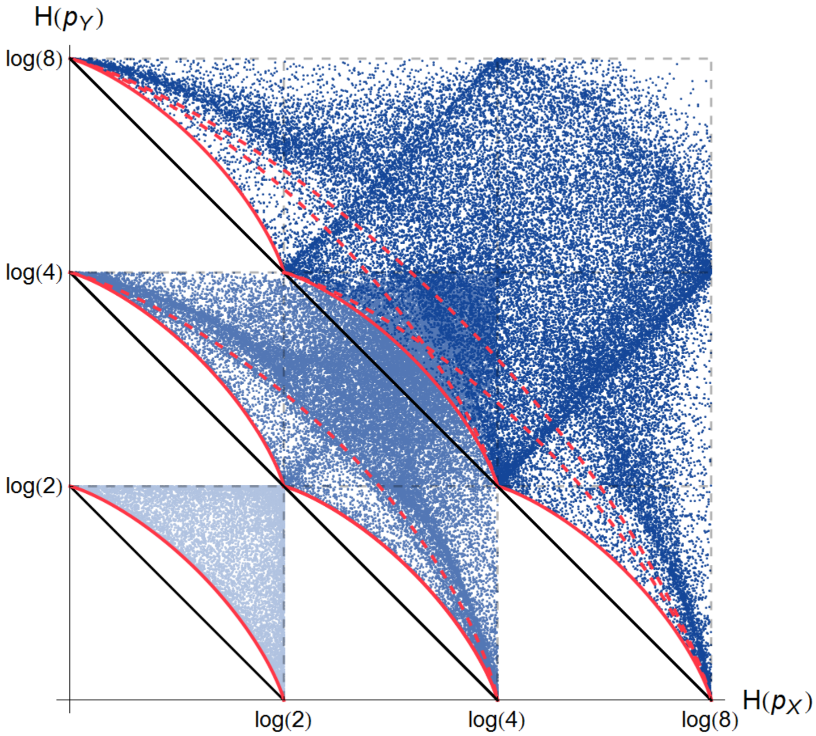

FIG. 8: Random sample of the entropy diagram for dimensions $d = 2$ (light shading), $d = 4$ (medium shading) and $d = 8$ (dark shading) for Fourier related observables and Shannon entropies. Our results falsify a previous conjecture by Englert *et al.* (dashed curves). Instead the optimal bounds are given by the solid curves, which are obtained by applying Conjecture V.6 and Conjecture V.7.

The consequence of this second conjecture is that, although the Fourier matrix can, in general, not be decomposed into a tensor product of Fourier matrices of smaller dimension, the entropy diagram (and hence the curve of minimal entropy pairs) does not change under this replacement. Hence, if this conjecture were true, we could apply Conjecture V.6 and characterize the curve of minimal entropy pairs by states of product form, where the marginals parametrize the optimal bound in the respective smaller dimension.

As an example let us consider Fourier related observables in dimension $d = 4$. Employing both conjectures we know that it suffices to consider only the problem of characterising the optimal bound for Fourier related observables in dimension $d = 2$. But for such observables we already characterized the bound completely (see Sect. V D) and, hence, the optimal bound in $d = 4$ is traced out by product states with marginals given by (63). Indeed, this result agrees with the random sample (FIG. 8). In FIG. 3 we also show other examples, where the numerics validate the two conjectures above.

Note that the above conjectures are statements about the case of composite dimension, effectively stating that for a large class of unitary operators one only needs to solve the problem in prime dimension. The prime-dimensional case, however, still remains a hard problem. But we can provide two further conjectures that, if correct, vastly reduce the complexity of calculating the optimal bound in these instances:

Conjecture V.8. *(Independence of the optimal states of* (α, β)*)*
If ρ *is an optimal state for any unitary operator and any* $\alpha, \beta > \frac{1}{2}$ *satisfying the duality relation* (2)*, then* ρ *is also an optimal state for all other dual pairs.*

This conjecture can be seen as an extension of Corollary IV.4. Note that we again excluded

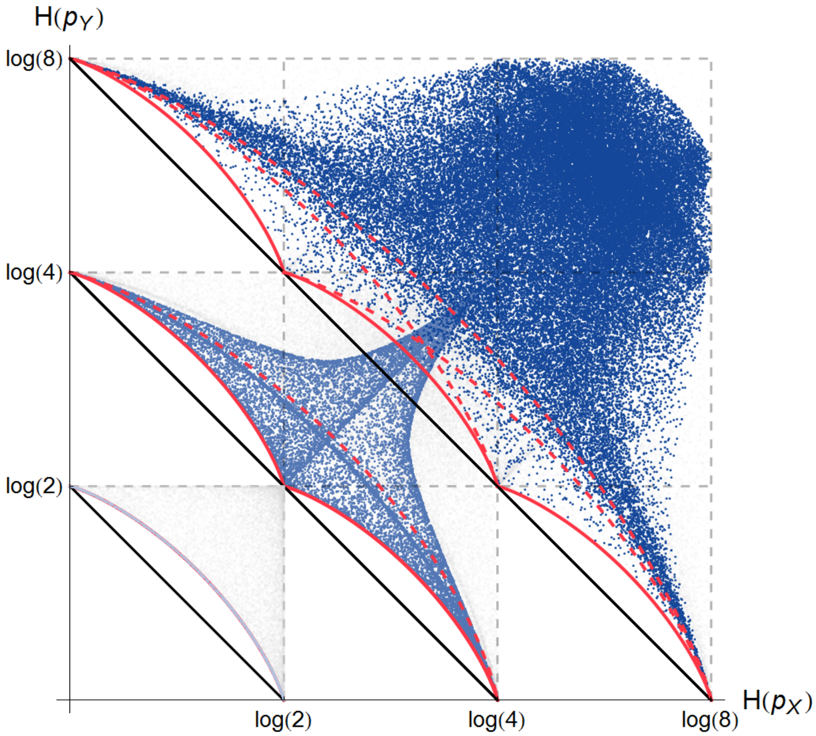

FIG. 9: Random sample of the entropy diagram for real-real symmetric states in dimensions $d = 2$ (light shading), $d = 4$ (medium shading) and $d = 8$ (dark shading) for Fourier related observables and Shannon entropies. Restricting to real-real symmetric states does not yield the complete entropy diagram (grey), but seems to be sufficient to characterize the optimal bound.

the extremal case $\{\alpha, \beta\} = \{1/2, \infty\}$ for the same reasons as explained in Sect. IV. In FIG. 4 the optimal bounds, although differently shaped, are traced out be the same states which supports Conjecture V.8.

The last conjecture only considers the case of observables linked by the Fourier matrix.

Conjecture V.9. *(Sufficiency of real-real symmetric states for Fourier)*
If ρ is an optimal state for the Fourier case, then there is a real-real symmetric state σ as given by (54) *with the same entropy pair.*

According to this conjecture it is sufficient to analyse the problem only for real-real symmetric states, which yields a huge simplification in both analytical and numerical treatments of the problem. As an example consider Fourier related observables in dimension $d = 3$. If Conjecture V.9 were correct, we already knew a characterisation of the optimal bound, since the real-real symmetric states in this case form a one-parameter family and therefore trace out the desired curve. Indeed, for $d = 3$ the real-real symmetric states coincide with the states conjectured by [8] which, as mentioned above, trace out the bound if we trust numerics. FIG. 9 also suggests the validity of Conjecture V.9.

Furthermore, we note that real-real symmetric states are closed under the tensor product, in the sense that any tensor product of two real-real symmetric states is again a real-real symmetric state. Hence, Conjecture V.6 and Conjecture V.9 agree with each other.

VI. CONCLUSION AND OUTLOOK

We investigated the curve of minimal entropies that completely describes the entropic uncertainty tradeoff between two observables. We showed that the lower bound on the sum of two entropies as given by the Maassen-Uffink uncertainty relation is not optimal in almost all cases and hence does not correspond to the curve of minimal entropies. To show this, we presented a novel proof of the MU bound that allowed us to analyse the case of equality in the uncertainty relation.

In order to characterize the curve of minimal entropies, we provided three main results: First, we showed that the optimal bound can be traced out by pure states. Second, the optimal bound for real-valued unitary operators can be traced out by real-valued pure states. And last, we presented an extremality criterion, which any optimal state must satisfy. Numerical and analytical results for the case of small dimension suggest a number of conjectures that, if true, lead to a drastic reduction of the optimisation space. The optimal lower bound could then be computed.

Acknowledgements

The work in Singapore is funded by the Singapore Ministry of Education (partly through the Academic Research Fund Tier 3 MOE2012-T3-1-009) and the National Research Foundation of Singapore. F.F. acknowledges support from LUH GRK 1463 and the Japan Society for the Promotion of Science (JSPS) by KAKENHI grant No. 24-02793. R.S. acknowledges support from the BMBF funded network Q.com-Q.

[1] W. Heisenberg. Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik. *Z. Phys.*, 43:172–198, 1927.

[2] E. H. Kennard. Zur Quantenmechanik einfacher Bewegungstypen. *Z. Phys.*, 44:326–352, 1927.

[3] H. Weyl. *Gruppentheorie und Quantenmechanik.* Hirzel, Leipzig, 1928.

[4] H. P. Robertson. The uncertainty principle. *Phys. Rev.*, 34:163–164, 1929.

[5] P. Busch, P. Lahti, and R. F. Werner. Measurement uncertainty relations. *J. Math. Phys.*, 55:042111, 2014. arXiv:1312.4392.

[6] P. J. Coles and F. Furrer. State-dependent approach to entropic measurement–disturbance relations. *Phys. Lett. A*, 379:105–112, 2015. arXiv:1311.7637.

[7] J. M. Renes and V. B. Scholz. Operationally-motivated uncertainty relations for joint measurability and the error-disturbance tradeoff. 2014. arXiv:1402.6711.

[8] B.-G. Englert, D. Kaszlikowski, L. C. Kwek, and W. H. Chee. Wave-particle duality in multi-path interferometers: General concepts and three-path interferometers. *Int. J. Quant. Inf.*, 6:129–157, 2008. arXiv:0710.0179.

[9] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner. Tight finite-key analysis for quantum cryptography. *Nature Commun.*, 3:634, 2012. arXiv:1103.4130.

[10] D. Deutsch. Uncertainty in quantum measurements. *Phys. Rev. Lett.*, 50:631–633, 1983.

[11] H. Maassen and J. B. M. Uffink. Generalized entropic uncertainty relations. *Phys. Rev. Lett.*, 60:1103–1106, 1988.

[12] M. Berta, M. Christandl, R. Colbeck, J. M. Renes, and R. Renner. The uncertainty principle in the presence of quantum memory. *Nature Phys.*, 2010. arXiv:0909.0950.

[13] I. D. Ivanovic. An inequality for the sum of entropies of unbiased quantum measurements. *J. Phys. A*, 25:L363, 1992.

[14] J. Sánchez-Ruiz. Improved bounds in the entropic uncertainty and certainty relations for complementary observables. *Phys. Lett. A*, 201:125–131, 1995.

[15] M. A. Ballester and S. Wehner. Entropic uncertainty relations and locking: tight bounds for mutually unbiased bases. *Phys. Rev. A*, 75, 2007. arXiv:quant-ph/0606244.

[16] Entropic uncertainty relation for mutually unbiased bases. 79.

[17] S. Wehner and A. Winter. Entropic uncertainty relations – a survey. *New J. Phys.*, 12:025009, 2010. arXiv:0907.3704.

[18] R. Adamczak, R. Latała, Z. Puchała, and K. Życzkowski. Asymptotic entropic uncertainty relations. 2014. arXiv:1412.7065.

[19] Z. Puchała, Ł. Rudnicki, and K. Życzkowski. Majorization entropic uncertainty relations. *J. Phys. A*, 46:272002, 2013. arXiv:1304.7755.

[20] Z. Puchała, Ł. Rudnicki, K. Chabuda, M. Paraniak, and K. Życzkowski. Certainty relations, mutual entanglement and non-displacable manifolds. 2015. arXiv:1506.07709.

[21] Ł. Rudnicki, Z. Puchała, and K. Życzkowski. Strong majorization entropic uncertainty relations. *Phys. Rev. A*, 89, 2014. arXiv:1402.0129.

[22] M. Krishna and K. R. Parthasarathy. An entropic uncertainty principle for quantum measurements. *Ind. J. Stat. A*, 64 No.3:842–852, 2001. arXiv:quant-ph/0110025.

[23] A. E. Rastegin. Rényi formulation of the entropic uncertainty principle for POVMs. *J. Phys. A*, 43:155302, 2010.

[24] P. J. Coles and M. Piani. Improved entropic uncertainty relations and information exclusion relations. *Phys. Rev. A*, 89, 2014. arXiv:1307.4265.

[25] S. Zozor, G. M. Bosyk, and M. Portesi. General entropy-like uncertainty relations in finite dimensions. *J. Phys. A*, 47:495302, 2014. arXiv:1311.5602.

[26] J. Sánches-Ruiz. Optimal entropic uncertainty relation in two-dimensional Hilbert space. *Phys. Lett. A*, 244:189–195, 1998.

[27] G. Ghirardi, L. Marinatto, and R. Romano. An optimal entropic uncertainty relation in a two-dimensional Hilbert space. *Phys. Lett. A*, 317:32–36, 2003.

[28] H. Maassen. The discrete entropic uncertainty relation. Talk given in Leyden University. Slides of a later version available from the author's website, 2007.

[29] P. J. Coles, L. Yu, and M. Zwolak. Relative entropy derivation of the uncertainty principle with quantum side information. 2011. arXiv:1105.4865.

[30] E. Phragmén and E. Lindelöf. Sur une extension d'un principe classique de l'analyse et sur quelques propriétés des fonctions monogènes dans le voisinage d'un point singulier. *Acta Math.*, 31:381–406, 1908.

[31] E. Hopf. A remark on linear elliptic differential equations of second order. *Proc. Amer. Math. Soc.*, 34(3):791–793, 1952.

[32] M. H. Protter and H. F. Weinberger. *Maximum principles in differential equations*. Springer, New York, 1984.

[33] K. Życzkowski. Complex hadamard matrices. Online catalogue, `http://chaos.if.uj.edu.pl/~karol/hadamard/`, 2003.

[34] W. Rudin. *Fourier Analysis on Groups*. John Wiley & Sons, 1962.

[35] J. A. Gallian. *Contemporary abstract algebra*. Brooks / Cole, cengage learning, 2006.