Entropic uncertainty principle for mixed states

Antonio F. Rotundo and René Schwonnek
Institut für Theoretische Physik, Leibniz Universität Hannover, 30167 Hannover, Germany

(Received 5 April 2023; accepted 18 April 2024; published 9 July 2024)

The entropic uncertainty principle in the form proven by Maassen and Uffink yields a fundamental inequality that is prominently used in many places all over the field of quantum information theory. In this paper, we provide a family of versatile generalizations of this relation. Our proof methods build on a deep connection between entropic uncertainties and interpolation inequalities for the doubly stochastic map that links probability distributions in two measurement bases. In contrast to the original relation, our generalization also incorporates the von Neumann entropy of the underlying quantum state. These results can be directly used to bound the extractable randomness of a source-independent quantum random number generator in the presence of fully quantum attacks, to certify entanglement between trusted parties, or to bound the entanglement of a system with an untrusted environment.

DOI: 10.1103/PhysRevResearch.6.033043

I. INTRODUCTION

Uncertainty relations express the limits imposed by quantum mechanics on our ability to either prepare a state with given properties, or measure the properties of a state to a given precision [1–4]. The study of uncertainty inequalities dates back to some of the most famous works of the early days of quantum theory [5–9] and has since then remained a topic of ongoing research [10–17]. Besides being an attractive rabbit hole on its own [18–27], having the right uncertainty relation at hand often proved to be a powerful tool [28–33], e.g., to build a worst-case model. For example, uncertainty relations commonly serve as an easy-to-establish estimate that allows determining, from measured data, properties such as the presence of entanglement [34–39], or the amount of extractable secure randomness [28,40–44].

In quantum information theory, uncertainty is typically quantified in terms of entropies. The prototype uncertainty relation of this type is due to an idea of Deutsch [45] and a conjecture by Kraus [46] proven by Maassen and Uffink [47]: Let X and Y denote two projective measurements, then the possible values of the Shannon entropies of their measurement outcomes, $H(X)$ and $H(Y)$, (measured on copies of a state ρ) are constraint by

$$H(X) + H(Y) \geqslant S(\rho) + c_{\text{KMU}}. \tag{1}$$

Here, c_{KMU} [see Eq. (7)] is a non-negative constant that depends on the overlap between the measurement bases of X and Y, and $S(\rho)$ is the von Neumann entropy of ρ.

In this paper, we establish a generalization of (1) to a family of entropic uncertainty relations of the form

$$\lambda H(X) + \mu H(Y) \geqslant \alpha S(\rho) + c_{XY}(\alpha, \lambda, \mu), \tag{2}$$

with parameters $\mu, \lambda, \alpha \in [0, 1]$. More precisely, we are interested in finding a constant $c_{XY}(\alpha, \lambda, \mu)$ such that (2) holds for all states ρ. Our main result, Theorem 1, provides this constant by drawing a connection to the norm of the doubly stochastic map that links the probability distributions in the X and the Y bases.

The von Neumann entropy term on the right-hand side (rhs) of (1) was not present in the original formulation of this inequality. It was however noted by Frank and Lieb [48,49] and Berta *et al.* [28], that it can be added without changing the constant c_{KMU}. An interesting consequence, which is often overlooked, is that a state that minimizes the gap of this inequality will not necessarily be pure. We extend this by including a weight α for the entropy term on the rhs of (2). The factor α sets the degree of mixedness that a state that minimizes the gap has. This goes from pure states that minimize the left-hand side (lhs) of (2) for $\alpha = 0$ (see Ref. [23]) to the maximally mixed state that saturates (2) for $\alpha = 2$ and $\mu + \lambda = 1$ with $c_{XY} = 0$. By this, we get a natural notion of a family of most certain (i.e., minimally uncertain) mixed states for measurements X and Y.

An uncertainty relation such as (2) can also be used to estimate the von Neumann entropy of an unknown state with given values of $H(X)$ and $H(Y)$, obtained, e.g., from measurement data. This has various practical applications. For example, consider the scenario in which a local system A, with a reduced state ρ_A, has interacted with an uncharacterized environment E. Here, (2) becomes handy for estimating correlations, since $S(\rho_A)$ describes the corresponding entanglement entropy. Building on this perspective, we demonstrate how to use our results for bounding the securely extractable randomness of a source-independent quantum random number generator, for attesting entanglement between two trusted parties, and between two trusted parties and an uncharacterized environment.

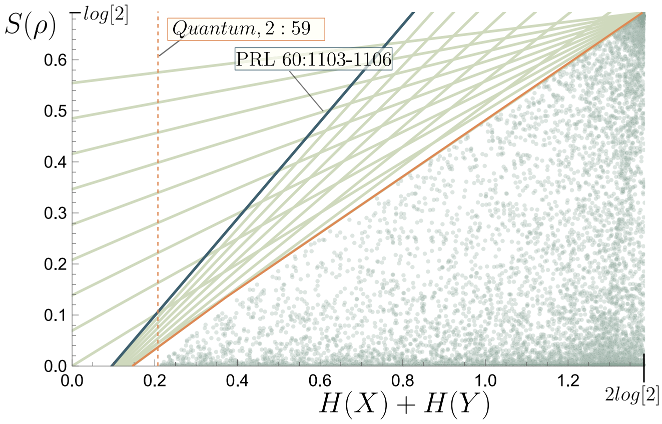

FIG. 1. Allowed regions of $[S(\rho), H(X)+H(Y)]$ tuples determined by random sampling over the state space (green dots), for $d = 2$ and measurements X and Y with a relative angle of 17°. The family of inequalities (2) determines linear bounds on this region (green lines). The uncertainty relation (1) from Ref. [47] corresponds to the blue line. Optimizing over our linear bounds (orange line) gives much stronger bounds.

II. PARAMETRIZED UNCERTAINTY RELATIONS

Including weights, such as α, λ, μ in (2), is a natural way of strengthening an existing relation. This has to be contrasted with many proposed *improvements* of the Maassen and Uffink relation that merely add more and more ρ-dependent terms to the rhs of (1).

One typical primordial question, preceding the use of an uncertainty relation, is to characterize the set of possible triples $\Omega_{XY} := \{(H(X), H(Y), S(\rho))\}_\rho$ that could be attained by a not further specified state ρ. Our result (2) directly serves this purpose by giving bounds on an arbitrary linear combination of $H(X)$, $H(Y)$, and $S(\rho)$. Given a valid value of c_{XY} for all parameters (α, μ, λ) allows for reconstructing a convex outer approximation to Ω_{XY} by performing a Legendre transformation [50] of c_{XY} with respect to α, λ, μ.

Another typical use of an uncertainty relation is to bound the value of one quantity given access to the others. The estimation of $S(\rho)$, mentioned above, is an example of this. Here, a given value of c_{XY} for a whole parameter range directly pays off when we use (2) to obtain the estimate

$$S(\rho) \leqslant \inf_{\lambda,\mu} \lambda H(X) + \mu H(Y) - c_{XY}(1, \lambda, \mu). \qquad (3)$$

In general, this gives stronger estimates than (1), which corresponds to evaluating the minimization above on the single point $\lambda = \mu = 1$.

The main result of this paper is the following theorem, which provides a closed form for c_{XY} in terms of operator norms:

Theorem 1. For measurements X and Y given by projectors $\{X_1, \ldots, X_{n_X}\}$ and $\{Y_1, \ldots, Y_{n_Y}\}$, consider the $n_X \times n_Y$ matrix $C^{(2)}$ with entries $C^{(2)}_{ij} = \mathrm{Tr}(X_i Y_j)$. For $0 \leqslant \lambda, \mu \leqslant \alpha$, we have

$$c_{XY}(\alpha, \lambda, \mu) \geqslant -\alpha \log \|C^{(2)}\|_{\frac{\alpha}{\mu} \to \frac{\alpha}{\alpha-\lambda}}. \qquad (4)$$

The norm appearing in the theorem is defined by

$$\|C^{(2)}\|_{r\to s} := \sup_{\phi \in \mathbb{C}^{n_Y}} \frac{\|C^{(2)}\phi\|_s}{\|\phi\|_r}, \qquad (5)$$

where $\|\cdot\|_p$ denotes the usual p-norm.

Plugging Eq. (4) in Eq. (2), we find

$$\lambda H(X) + \mu H(Y) \geqslant \alpha S(\rho) - \alpha \log \|C^{(2)}\|_{\frac{\alpha}{\mu}\frac{\alpha}{\alpha-\lambda}}. \qquad (6)$$

A. Evaluating the norm

In principle, the operator norm in the above can be computed numerically. A discussion on this with a focus on known hardness results for general matrices can be found in Refs. [51,52]. An easy-to-use and in most instances also robust seesaw method can be found in Chap. 6.2 of Ref. [51]. However, this method does not come with an accuracy guarantee. In critical applications such as cryptography we therefore have to employ other methods such as hierarchies of semidefinite programming (SDP) relaxations [53] or the algorithm described in Ref. [54]. In any case, computing (5) for large system sizes and an unstructured $C^{(2)}$ may likely turn out to be challenging in practice. Therefore, we provide some analytical results and a conjecture that drastically simplify this computation.

At one end of the parameter range, we have the limit $\mu \to \alpha$. In this case $(r = 1)$, computing the norm in (6) becomes straightforward since Eq. (5) is a convex optimization over a polytope. Moreover, an additional limit $\lambda \to \alpha$ will recover the well-known result of Kraus, Maassen, and Uffink (KMU) [46,47],

$$\|C^{(2)}\|_{1\to\infty} = \max_{ij} C^{(2)}_{ij}. \qquad (7)$$

At the other end of the parameter range we have the limit $\lambda, \mu \to 0$ for α fixed. Here, the lhs of (2) will vanish and the optimal bound is attained for the maximally mixed state with a constant $c_{XY} = -\alpha \log(d)$, which also coincides with the bound given by Theorem 1.

By inspecting the typical behavior of linear uncertainty inequalities (2) for further parameters starting from this point $(\mu = \lambda = 0)$, it becomes clear that there is in fact a large part of the parameter range where an optimal linear bound is saturated by the maximally mixed state.

Note that the resulting bounds are nevertheless nontrivial and can actually provide a quite good characterization of the set Ω_{XY}. This can be seen for example by the fact that the well-known bound (1) falls into this category when X and Y are mutually unbiased. A solid geometrical intuition for this observation can be drawn from a diagram as in Fig. 1. Here, the bounds given by (2) correspond to lines whose slopes are determined by the ratios between the parameters α, μ, and λ. The intercepts of these lines are determined by the value of $c_{XY}(\alpha, \lambda, \mu)$. A line with an optimal constant $c_{XY}(\alpha, \lambda, \mu)$ will touch the set of attainable points (here sampled by green dots). For an almost triangular-shaped set (as in the example) it is typical that most optimal lines will "touch" the most upper right point. This point corresponds to the maximally mixed state and has coordinates $[(\lambda + \mu)\log(d), \alpha \log(d)]$.

In the Supplemental Material (SM) [55] we check that our bound (6) is indeed tight for states in a small environment around the maximally mixed state and will therefore give the optimal uncertainty bound when a relation is saturated in this parameter regime. Furthermore, computing the norm in Theorem 1 becomes easy in this situation (see Sec. C in SM [55])

Under the assumption that the set Ω_{XY} is star shaped with the point $((\lambda+\mu)\log(d), \alpha\log(d))$ as the center, we can give a characterization of the parameter range for which (2) will saturate on the maximally mixed state [55]. This leads us to the following statement:

Conjecture 1. Let σ_2 denote the second largest singular value of $C^{(2)}$. For parameters obeying

$$\frac{\alpha-\mu}{\mu}\frac{\alpha-\lambda}{\lambda} \geqslant \sigma_2^2, \tag{8}$$

we have the optimal uncertainty relation

$$\lambda H(X) + \mu H(Y) \geqslant \alpha S(\rho) - (\alpha-\lambda-\mu)\log d. \tag{9}$$

Strong evidence supporting this conjecture is given in SM [55]. In particular, notice that the conjecture certainly holds for mutually unbiased bases (MUBs), and can be easily proven for $\lambda+\mu \leqslant \alpha$ and for qubits. Note that the part of this conjecture that could break down is (8). As a consequence (9) will still hold, but in a smaller parameter range. One can use the result of Sec. D in SM [55] to obtain numerically an upper bound on this range without invoking the conjecture.

Below, we will consider different applications of Eq. (6), and use the analytical expression given by Eq. (9) to find optimal values for μ and λ. For critical applications, such as security proofs, one has however to check the validity of the analytical expression, for that specific point, by numerically evaluating the norm.

B. Comparison to existing uncertainty relations

In this section, we compare (6) with two other known existing uncertainty relations (EURs): that of Ref. [28], which we denote BCCRR,

$$H(X) + H(Y) \geqslant S(\rho) - \log c_1, \tag{10}$$

and the inequality RPZ$_2$ from Ref. [18],

$$H(X) + H(Y) \geqslant S(\rho) - \log[c_1 C^2 + c_2(1-C^2)]. \tag{11}$$

Here, following Ref. [18], c_1 and c_2 denote the first and second largest elements of $C^{(2)}$, and $C \equiv (1+\sqrt{c_1})/2$.

To compare with these inequalities, which give equal weights to $H(X)$ and $H(Y)$, we set $\mu=\lambda$ and $\alpha=1$. Using Conjecture 1 and setting μ to saturate Eq. (8), we find

$$H(X) + H(Y) \geqslant (1+\sigma_2)S(\rho) + (1-\sigma_2)\log d. \tag{12}$$

The entropy term in Eq. (12) is always larger than in both BCCRR and RPZ$_2$. Therefore, in our comparison, we consider only the second, state-independent, term.

We first consider $d=2$. In this case, the most general $C^{(2)}$ matrix is given by

$$C^{(2)} = \begin{pmatrix} \cos^2\theta & \sin^2\theta \\ \sin^2\theta & \cos^2\theta \end{pmatrix}, \quad \theta \in [0, \pi/4], \tag{13}$$

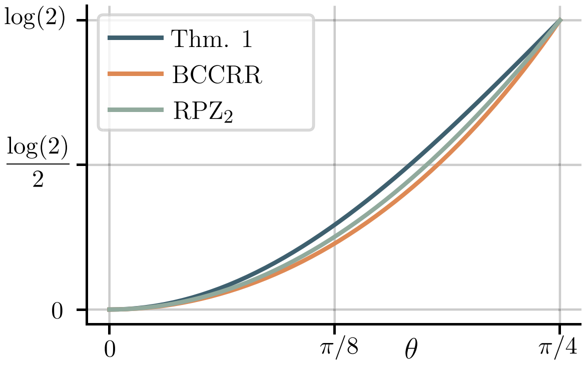

FIG. 2. Comparison of the state-independent bound provided by BCCRR. RPZ$_2$, and Eq. (12) for $d=2$. The angle θ parametrizes $C^{(2)}$, as in Eq. (13).

where $\theta=0$ corresponds to $X=Y$, and $\theta=\pi/4$ to the MUB case. The bounds provided by BCCRR, RPZ$_2$, and Eq. (12) are compared in Fig. 2. The bounds are equivalent for $\theta=0$ and $\theta=\pi/4$, while in between our bound is stronger.

For $d>2$, the matrices $C^{(2)}$ have too many parameters, and we cannot scan them all, as we did in Fig. 2. Instead, we compare our bound, Eq. (12), to BCCRR and RPZ$_2$ for some random $C^{(2)}$, generated by setting $C^{(2)}_{ij} = |U_{ij}|^2$, where U is a Haar random unitary. In Fig. 3, we plot the percentage of $C^{(2)}$ for which our bound is better than BCCRR or RPZ$_2$ as a function of d. As expected, for $d=2$, our bound is always at least as good as both BCCRR and RPZ$_2$. The percentage of $C^{(2)}$ for which our bound is better decreases for $d=3,4$, but then starts increasing. For $d \gg 1$, our bound is equivalent or better with a probability that approaches 1.

III. PRACTICAL APPLICATIONS

From the comparison above, we know that Eq. (6), for $\mu=\lambda$, provides stronger constraints compared to other EURs for many observables X and Y [Eq. (12)]. Therefore, it can be useful in all applications of other EURs. However, imposing $\mu=\lambda$ we lose part of the power of Eq. (6), i.e., that of giving different weights to $H(X)$ and $H(Y)$. This is often beneficial in practical applications, as we show

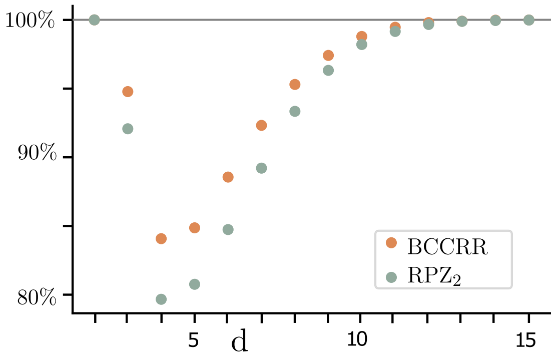

FIG. 3. Percentage of $C^{(2)}$ for which our bound is better than BCCRR or RPZ, as a function of d. We have used a sample of 10^5 random $C^{(2)}$.

in three examples: bounding extractable randomness, entanglement detection, and bounding entanglement with an eavesdropper.

A. Bounding extractable randomness

Quantum random number generators will likely be one of the first competing market-ready quantum devices. However, proving their security without imposing too strong assumptions is still under development. A promising class of protocols are source-independent random number generators. Their basic security mechanism can be traced back to the use of the uncertainty relation (1). Our results can be directly used to get stronger bounds on the extractable randomness.

In a basic protocol [56], we are provided with a state ρ, emitted by an untrusted source, from which we want to extract random numbers. We are allowed to perform measurements X and Y. By convention, the X measurement will be used for generating a secret number. The entropy $H(Y)$ of the other measurement, in this context usually referred to as the phase-error rate, will be used to certify properties of ρ. We consider fully quantum attacks, modeled by granting an adversary E full access to the purification of ρ.

It was shown in Refs. [57,58] that the single-shot quantity that has to be bounded for estimating the rate of securely extractable randomness (both asymptotically and finite) is given by the conditional entropy $H(X|E)$, which in our case can equivalently [59] be computed by $H(X) - S(\rho)$. Using (6), we can bound this expression as

$$H(X|E) \geqslant \max_{\mu,\lambda}\,(1-\lambda)H(X) - \mu H(Y) - \log \|C^{(2)}\|. \quad (14)$$

The main advantage of using Eq. (6) is that we can optimize over μ and λ to obtain improved bounds compared to other symmetric EURs. The optimal value can be found by numerically evaluating the norm.

Using Conjecture 1, we can avoid numerics and get an analytical bound. Let $\Delta_X \equiv \log d - H(X)$, $\Delta_Y \equiv \log d - H(Y)$, then one can show that, as long as (8) is satisfied, the optimal bound is [55]

$$H(X|E) \geqslant \begin{cases} \frac{(\sqrt{\Delta_Y}-\sigma_2\sqrt{\Delta_X})^2}{1-\sigma_2^2}, & \gamma \geqslant \sigma_2, \\ \Delta_Y - \Delta_X, & \gamma < \sigma_2, \end{cases} \quad (15)$$

where $\gamma \equiv \sqrt{\Delta_X/\Delta_Y}$. Notice that without loss of generality we can assume that $\gamma \leqslant 1$ (swap X and Y if this is not the case).

B. Entanglement detection

Consider now a bipartite state ρ_{AB}, shared between two parties, A and B, that can perform local measurements, $X_{AB} = X_A \otimes X_B$, $Y_{AB} = Y_A \otimes Y_B$, and exchange classical information. To use Eq. (6) for detecting entanglement, we follow Ref. [32]; one can show that ρ_{AB} is entangled if [55]

$$\lambda H(X_{AB}) + \mu H(Y_{AB}) < S_{\max} - \log \left\|C_A^{(2)}\right\| \left\|C_B^{(2)}\right\|. \quad (16)$$

Here, $S_{\max} = \max[S(\rho_A), S(\rho_B)]$.

We can use Conjecture 1 to find a condition that is easier to treat analytically. Let $\sigma_2 = \max(\sigma_{2,A}, \sigma_{2,B})$, where $\sigma_{2,A}$ and $\sigma_{2,B}$ are the second largest singular values of $C_A^{(2)}$ and $C_B^{(2)}$. Then, as long as μ, λ obey Eq. (8), we find that ρ_{AB} is entangled if

$$\lambda\Delta_X + \mu\Delta_Y > \log d - S_{\max}. \quad (17)$$

Here, $\Delta_X \equiv \log d - H(X_{AB})$, $\Delta_Y \equiv \log d - H(Y_{AB})$, and $d = d_A d_B$ is the total size of the Hilbert space. Since both Δ_X and Δ_Y are non-negative, the best we can do is to take μ and λ as big as possible. However, the constraints (8) prevent us from increasing μ and λ independently. The optimal value of (μ, λ) for given $\Delta_{X,Y}$ is [55]

$$\mu = \frac{1-\sigma_2\gamma}{1-\sigma_2^2}, \quad \lambda = \frac{1-\sigma_2/\gamma}{1-\sigma_2^2}, \quad \gamma \equiv \sqrt{\frac{\Delta_X}{\Delta_Y}}, \quad (18)$$

if $\sigma_2 \leqslant \gamma \leqslant 1/\sigma_2$. When $\gamma < \sigma_2$, the optimal choice is $(\mu, \lambda) = (1, 0)$, and, when $\gamma > 1/\sigma_2$, it is $(\mu, \lambda) = (0, 1)$. In the original notation, in terms of $H(X)$ and $H(Y)$, we find that, for $\sigma_2 \leqslant \gamma \leqslant 1/\sigma_2$, ρ_{AB} is entangled if

$$H(X_{AB}) + H(Y_{AB}) < \left(1-\sigma_2^2\right)S_{\max} + \left(1+\sigma_2^2\right) \times \log d - 2\sigma_2\sqrt{\Delta_X\Delta_Y}. \quad (19)$$

We conclude that the freedom of keeping $\mu \neq \lambda$ generally helps.

C. Bound on entropy

Consider the same setup as in the entanglement detection example; A and B are now interested in quantifying how much entanglement they might share with an eavesdropper, E. Let ρ_{ABE} be the joint state of A, B, and E; in the worst case, this state is pure, and $S(\rho_E) = S(\rho_{AB})$. A direct application of Eq. (6) gives the following bound:

$$S(E) \leqslant \min_{\mu,\lambda} \lambda H(X_{AB}) + \mu H(Y_{AB}) + \log \left\|C_{AB}^{(2)}\right\|. \quad (20)$$

To obtain an analytic result, we can again use our conjecture, and proceed similarly to what we did above for entanglement detection. As long as $\sigma_2 \leqslant \gamma \leqslant 1/\sigma_2$, we find that the optimal choices for μ and λ are again given by (18), where σ_2 is now the second largest singular value of $C_{AB}^{(2)}$. We arrive at the following improved bound for $S(E)$,

$$S(E) \leqslant \frac{1}{1-\sigma_2^2}\Big[H(X) + H(Y) + 2\sqrt{\Delta_X\Delta_Y}\sigma_2 - \left(1+\sigma_2^2\right)\log d_A d_B\Big]. \quad (21)$$

Notice that, for MUB, we find again that the best we can do is to set $\mu = \lambda = 1$.

IV. CONCLUSIONS

In this paper, we have introduced a class of EURs, Eq. (6), which allows giving different weights to $H(X)$, $H(Y)$, and $S(\rho)$. We have shown that these EURs often provide better bounds than other EURs known in the literature. Moreover, we have shown in three examples that the freedom of giving different weights can be helpful in practical applications. Equation (6) is expressed in terms of norms, which are difficult to estimate numerically. We have explored properties of these norms, and formulated a conjecture that, if correct, leads to an analytic result valid for most of the parameter space. In particular, we have obtained Eq. (12), that provides a simple alternative to Maassen-Uffink, where $\log c_{\mathrm{MU}}$ is replaced by $(1 - \sigma_2)\log d$.

There are several directions in which this work could be extended. Clearly, it would be nice to prove Conjecture 1. Also, using Conjecture 1, we can analytically study Eq. (6) for values of (μ, λ) satisfying Eq. (8). Close to $\mu = \lambda = 1$, the KMU result applies. It remains to explore Eq. (6) for intermediate values of (μ, λ). Finally, for applications to quantum key distribution, it would be interesting to extend Eq. (6) to Renyi and conditional entropies.

ACKNOWLEDGMENTS

We gratefully acknowledge discussions with Mario Berta, Giovanni Chesi, Thomas Cope, Andreea Lefterovici, Lorenzo Maccone, Tobias Osborne, Marco Tomamichel, and Henrik Wilming. A.R. thanks the Quantum Information Theory Group (QUit) of the University of Pavia for hospitality during the completion of this work. We are very grateful to Frits Verhagen for pointing out a missing argument in an earlier version of the proof of Theorem 1. We also have to thank an unknown referee for spotting a sign mistake and an unexplained notation in the same proof. Fortunately both issues could be easily fixed. A.R. acknowledges financial support by the Bundesministerium für Bildung und Forschung (BMBF) project QuBRA. R.S. acknowledges financial support by the Quantum Valley Lower Saxony and by the BMBF project ATIQ.

[1] R. Schwonnek, D. Reeb, and R. F. Werner, Measurement uncertainty for finite quantum observables, Mathematics **4**, 38 (2016).

[2] A. Barchielli, M. Gregoratti, and A. Toigo, Measurement uncertainty relations for discrete observables: Relative entropy formulation, Commun. Math. Phys. **357**, 1253 (2018).

[3] P. Busch, P. Lahti, and R. F. Werner, Measurement uncertainty relations, J. Math. Phys. **55**, 042111 (2014).

[4] P. Busch, P. Lahti, and R. F. Werner, Proof of Heisenberg's error-disturbance relation, Phys. Rev. Lett. **111**, 160405 (2013).

[5] W. Heisenberg, Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik, Z. Phys. **43**, 172 (1927).

[6] E. Schrödinger, Die gegenwärtige Situation in der Quantenmechanik, Naturwiss. **23**, 807 (1935).

[7] H. Weyl, *Gruppentheorie und Quantenmechanik* (Hirzel, Leipzig, 1928).

[8] H. P. Robertson, The uncertainty principle, Phys. Rev. **34**, 163 (1929).

[9] E. H. Kennard, Zur Quantenmechanik einfacher Bewegungstypen, Z. Phys. **44**, 326 (1927).

[10] I. I. Hirschman, A note on entropy, Am. J. Math. **79**, 152 (1957).

[11] A. Riccardi, C. Macchiavello, and L. Maccone, Tight entropic uncertainty relations for systems with dimension three to five, Phys. Rev. A **95**, 032109 (2017).

[12] A. Riccardi, C. Macchiavello, and L. Maccone, Multipartite steering inequalities based on entropic uncertainty relations, Phys. Rev. A **97**, 052307 (2017).

[13] P. J. Coles and F. Furrer, State-dependent approach to entropic measurement–disturbance relations, Phys. Lett. A **379**, 105 (2015).

[14] G. Sharma, C. Mukhopadhyay, S. Sazim, and A. K. Pati, Quantum uncertainty relation based on the mean deviation, Phys. Rev. A **98**, 032106 (2018).

[15] S. Wehner and A. Winter, Entropic uncertainty relations – a survey, New J. Phys. **12**, 025009 (2010).

[16] P. Coles, M. Berta, M. Tomamichel, and S. Wehner, Entropic uncertainty relations and their applications, Rev. Mod. Phys. **89**, 015002 (2017).

[17] L. Gao, M. Junge, and N. LaRacuente, Uncertainty principle for quantum channels, in *2018 IEEE International Symposium on Information Theory (ISIT)* (IEEE, New York, 2018), pp. 996–1000.

[18] Ł. Rudnicki, Z. Puchała, and K. Życzkowski, Strong majorization entropic uncertainty relations, Phys. Rev. A **89**, 052115 (2014).

[19] A. A. Abbott and C. Branciard, Noise and disturbance of qubit measurements: An information-theoretic characterization, Phys. Rev. A **94**, 062110 (2016).

[20] C. de Gois, K. Hansenne, and O. Gühne, Uncertainty relations from graph theory, Phys. Rev. A **107**, 062211 (2023).

[21] R. Schwonnek, Additivity of entropic uncertainty relations, Quantum **2**, 59 (2018).

[22] K. Szymański and K. Życzkowski, Geometric and algebraic origins of additive uncertainty relations, J. Phys. A: Math. Theor. **53**, 015302 (2020).

[23] K. Abdelkhalek, R. Schwonnek, H. Maassen, F. Furrer, J. Duhme, P. Raynal, B. G. Englert, and R. F. Werner, Optimality of entropic uncertainty relations, Int. J. Quantum Inf. **13**, 1550045 (2015).

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

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

[26] B.-F. Xie, F. Ming, D. Wang, L. Ye, and J.-L. Chen, Optimized entropic uncertainty relations for multiple measurements, Phys. Rev. A **104**, 062204 (2021).

[27] D. Wang, F. Ming, M.-L. Hu, and L. Ye, Quantum-memory-assisted entropic uncertainty relations, Anna. Phys. **531**, 1900124 (2019).

[28] M. Berta, M. Christandl, R. Colbeck, J. M. Renes, and R. Renner, The uncertainty principle in the presence of quantum memory, Nat. Phys. **6**, 659 (2010).

[29] J. Schneeloch, C. J. Broadbent, S. P. Walborn, E. G. Cavalcanti, and J. C. Howell, Einstein-Podolsky-Rosen steering inequalities from entropic uncertainty relations, Phys. Rev. A **87**, 062103 (2013).

[30] M. A. Ballester and S. Wehner, Entropic uncertainty relations and locking: Tight bounds for mutually unbiased bases, Phys. Rev. A **75**, 022319 (2007).

[31] B. Lücke, J. Peise, G. Vitagliano, J. Arlt, L. Santos, G. Tóth, and C. Klempt, Detecting multiparticle entanglement of Dicke states, Phys. Rev. Lett. **112**, 155304 (2014).

[32] A. Riccardi, G. Chesi, C. Macchiavello, and L. Maccone, Tight bounds from multiple-observable entropic uncertainty relations, Ann. Phys., 2400020 (2024).

[33] A. C. S. Costa, R. Uola, and O. Gühne, Steering criteria from general entropic uncertainty relations, Phys. Rev. A **98**, 050104(R) (2018).

[34] O. Gühne and G. Tóth, Entanglement detection, Phys. Rep. **474**, 1 (2009).

[35] O. Gühne, Detecting quantum entanglement: entanglement witnesses and uncertainty relations, Ph.D. thesis, Universität Hannover, 2004.

[36] H. F. Hofmann and S. Takeuchi, Violation of local uncertainty relations as a signature of entanglement, Phys. Rev. A **68**, 032103 (2003).

[37] R. Schwonnek, L. Dammeier, and R. F. Werner, State-independent uncertainty relations and entanglement detection in noisy systems, Phys. Rev. Lett. **119**, 170404 (2017).

[38] B. Bergh and M. Gärttner, Experibmentally accessible bounds on distillable entanglement from entropic uncertainty relations, Phys. Rev. Lett. **126**, 190503 (2021).

[39] T. Kriváchy, F. Fröwis, and N. Brunner, Tight steering inequalities from generalized entropic uncertainty relations, Phys. Rev. A **98**, 062111 (2018).

[40] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, Tight finite-key analysis for quantum cryptography, Nat. Commun. **3**, 634 (2012).

[41] M. Masini, S. Pironio, and E. Woodhead, Simple and practical DIQKD security analysis via BB84-type uncertainty relations and Pauli correlation constraints, Quantum **6**, 843 (2022).

[42] F. Grasselli, G. Murta, H. Kampermann, and D. Bruß, Entropy bounds for multiparty device-independent cryptography, PRX Quantum **2**, 010308 (2021).

[43] R. Schwonnek, K. T. Goh, I. W. Primaatmaja, E. Y.-Z. Tan, R. Wolf, V. Scarani, and C. C.-W. Lim, Device-independent quantum key distribution with random key basis, Nat. Commun. **12**, 2880 (2021).

[44] W. Zhang, T. V. Leent, K. Redeker, R. Garthoff, R. Schwonnek, F. Fertig, S. Eppelt, W. Rosenfeld, V. Scarani, C. C.-W. Lim *et al.*, A device-independent quantum key distribution system for distant users, Nature (London) **607**, 687 (2022).

[45] D. Deutsch, Uncertainty in quantum measurements, Phys. Rev. Lett. **50**, 631 (1983).

[46] K. Kraus, Complementary observables and uncertainty relations, Phys. Rev. D **35**, 3070 (1987).

[47] H. Maassen and J. B. M. Uffink, Generalized entropic uncertainty relations, Phys. Rev. Lett. **60**, 1103 (1988).

[48] H. Maassen, A discrete entropic uncertainty relation, in *Quantum Probability and Applications V*, edited by L. Accardi and W. von Waldenfels, Lecture Notes in Mathematics, Vol. 1442 (Springer, Berlin, 1990), pp. 263–266.

[49] R. L. Frank and E. H. Lieb, Entropy and the uncertainty principle, Ann. Henri Poincaré **13**, 1711 (2012).

[50] L. Dammeier, R. Schwonnek, and R. F. Werner, Uncertainty relations for angular momentum, New J. Phys. **9**, 093046 (2015).

[51] R. Schwonnek, Uncertainty relations in quantum theory, Ph.D. thesis, Leibniz University Hannover, 2018, https://doi.org/10.15488/3600.

[52] V. Bhattiprolu, M. K. Ghosh, V. Guruswami, E. Lee, and M. Tulsiani, Inapproximability of matrix norms, SIAM J. Comput. **52**, 132 (2023).

[53] J. B. Lasserre, *Moments, Positive Polynomials and Their Applications* (World Scientific, Singapore, 2009), Vol. 1.

[54] V. Bhattiprolu, M. Ghosh, V. Guruswami, E. Lee, and M. Tulsiani, Approximating operator norms via generalized Krivine rounding, arXiv:1804.03644.

[55] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevResearch.6.033043 for proofs of the various statements and some additional results, which includes Refs. [60–63].

[56] Z. Cao, H. Zhou, X. Yuan, and X. Ma, Source-independent quantum random number generation, Phys. Rev. X **6**, 011020 (2016).

[57] R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner, and T. Vidick, Practical device-independent quantum cryptography via entropy accumulation, Nat. Commun. **9**, 459 (2018).

[58] R. Renner, Security of quantum key distribution, Int. J. Quantum Inf. **06**, 1 (2008).

[59] E. Y.-Z. Tan, R. Schwonnek, K. T. Goh, I. W. Primaatmaja, and C. C.-W. Lim, Computing secure key rates for quantum cryptography with untrusted devices, npj Quantum Inf. **7**, 158 (2021).

[60] S. Golden, Lower bounds for the Helmholz function, Phys. Rev. **137**, B1127 (1965).

[61] C. J. Thompson, inequality with applications in statistical mechanics, J. Math. Phys. **6**, 1812 (1965).

[62] A. Bhaskara and A. Vijayaraghavan, Approximating matrix p-norms, in *Proceedings of the Twenty-Second Annual ACM-SIAM Symposium on Discrete Algorithms* (SIAM, Philadelphia, 2011), pp. 497–511.

[63] R. F. Werner, Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model, Phys. Rev. A **40**, 4277 (1989).