Improved bounds on entropic uncertainty relations

Julio I. de Vicente[1] and Jorge Sánchez-Ruiz[1,2]
[1]*Departamento de Matemáticas, Universidad Carlos III de Madrid, Avenida de la Universidad 30, 28911 Leganés, Madrid, Spain*
[2]*Instituto Carlos I de Física Teórica y Computacional, Universidad de Granada, 18071 Granada, Spain*
(Received 25 September 2007; published 16 April 2008)

Entropic uncertainty relations place nontrivial lower bounds to the sum of Shannon information entropies for noncommuting observables. Here we obtain a lower bound on the entropy sum for general pairs of observables in finite-dimensional Hilbert space, which improves on the best bound known to date [H. Maassen and J. B. M. Uffink, Phys. Rev. Lett. **60**, 1103 (1988)] for a wide class of observables. This result follows from another formulation of the uncertainty principle, the Landau-Pollak inequality, whose relationship to the Maassen-Uffink entropic uncertainty relation is discussed.

DOI: 10.1103/PhysRevA.77.042110 PACS number(s): 03.65.Ta, 03.67.−a

I. INTRODUCTION

The uncertainty principle states that for quantum systems there is an irreducible lower bound on the uncertainty in the result of simultaneous measurements for general pairs of noncommuting observables. This is one of the key aspects of quantum mechanics, since it is one of the fundamental points of departure of the theory with respect to classical physics.

The oldest and most widely used mathematical formulation of the uncertainty principle is the Heisenberg-Robertson uncertainty relation [1], which places a lower bound on the product of the standard deviations for any pair of noncommuting observables. However, two decades ago several authors [2,3] pointed out that this inequality actually fails to express properly the physical contents of the uncertainty principle, and proposed to use instead the so-called entropic uncertainty relations (EURs), which place lower bounds to the sum of the Shannon information entropies of observables. In fact, for the position-momentum and angle-angular momentum pairs the optimal (i.e., sharpest) EURs were already found in Ref. [4], while in finite-dimensional Hilbert space several EURs have been derived for general pairs of observables [2,5–7], as well as for particular sets of more than two observables such as the so-called complementary observables [8].

Recently, EURs in the finite-dimensional setting have been proved to be not only a subject of fundamental importance, as a completely rigorous mathematical formulation of the uncertainty principle, but also a useful tool in quantum information theory. For instance, EURs have been used to derive separability criteria [9], to show the possibility of locking classical correlations in quantum states [10], and to prove the security of protocols of quantum cryptography [11]. Unfortunately, the EURs obtained so far for observables in finite-dimensional Hilbert space are not completely tight in general, and the optimal lower bound on the entropy sum is only known in a few special cases. Our aim in this paper is to improve on the best bound known to date for general pairs of observables acting on a Hilbert space of arbitrary finite dimension [6].

Let A and B denote two Hermitian operators representing physical observables in an N-dimensional Hilbert space, with respective complete orthonormal sets of eigenvectors $\{|a_i\rangle\}$ and $\{|b_i\rangle\}$ $(i=1,\ldots,N)$, and let $|\psi\rangle$ denote the normalized state vector describing the quantum (pure) state of the system. For the sake of simplicity, we assume that both A and B have nondegenerate spectra, so that there are N possible outcomes for measurements of each observable and the probabilities $p_i(A,\psi)$, $p_i(B,\psi)$ $(i=1,\ldots,N)$ are given by

$$p_i(A,\psi)=|\langle\psi|a_i\rangle|^2, \quad p_i(B,\psi)=|\langle\psi|b_i\rangle|^2. \tag{1}$$

An entropic uncertainty relation (EUR) for the pair A,B is an inequality of the form

$$H_\psi(A)+H_\psi(B)\geq H_{AB}>0, \tag{2}$$

where $H_\psi(X)$ is the Shannon information entropy corresponding to the probability distribution $\{p_i(X,\psi)\}$,

$$H_\psi(X)=-\sum_{i=1}^{N} p_i(X,\psi)\ln p_i(X,\psi). \tag{3}$$

According to Shannon's information theory [12], entropy is the only rigorous quantitative measure of the uncertainty or lack of information associated to a random variable. The EUR (2) thus sets a nontrivial lower bound, the positive constant H_{AB}, to the joint (information-theoretic) uncertainty about the outcomes of simultaneous measurements of A and B in any quantum state [13].

As first shown by Deutsch [2], an inequality of the form (2) does indeed exist for any pair of observables that do not share any common eigenstate, as must be expected from a satisfactory quantitative expression of the uncertainty principle. Specifically, in Ref. [2], Deutsch proved that

$$H(A)+H(B)\geq -2\ln\left(\frac{1+c}{2}\right), \tag{4}$$

where

$$c=c(A,B)\equiv\max_{i,j}|\langle a_i|b_j\rangle| \tag{5}$$

is usually called the overlap of observables A and B (notice that $1/\sqrt{N}\leq c\leq 1$ in N-dimensional Hilbert space). The Deutsch EUR (4) was later improved by Maassen and Uffink [6], who showed that

$$H(A) + H(B) \geq -2 \ln c. \tag{6}$$

This inequality is the sharpest EUR known to date for a general pair of observables in finite-dimensional Hilbert space. In the particular case when A and B are complementary observables [5,14], i.e., $|\langle a_i|b_j\rangle| = 1/\sqrt{N}$ for all $i,j = 1,\ldots,N$, the lower bound $\ln N$ given by Eq. (6) is optimal since it is attained whenever the system is in an eigenstate of either A or B [5]. Leaving aside this special case, however, the Maassen-Uffink EUR is not optimal, in the sense that the lower bound (6) is not attained for any quantum state. The problem of finding the optimal EUR for general (noncomplementary) observables turns out to be very difficult, and up to now it has only been solved in two-dimensional Hilbert space [7].

Another alternative mathematical formulation of the uncertainty principle is provided by the Landau-Pollak uncertainty relation, which states that

$$\arccos\sqrt{P_A} + \arccos\sqrt{P_B} \geq \arccos c, \tag{7}$$

where

$$P_A \equiv \max_i p_i(A), \quad P_B \equiv \max_j p_j(B). \tag{8}$$

This inequality was first considered in the quantum setting by Uffink [6,15], who adapted the original work of Landau and Pollak on uncertainty in signal theory [16]. It satisfies some of the formal requirements proposed by Deutsch [2] to characterize general uncertainty relations, and has been used to derive separability conditions in the framework of quantum information theory [17]. Remarkably, Eq. (7) is neither weaker nor stronger than Eq. (6), since one can find probability distributions allowed by the latter but forbidden by the former, and vice versa [15]. However, the Landau-Pollak inequality does not provide a completely satisfactory expression of the uncertainty principle, for example because the uncertainty functional in the left-hand side of Eq. (7) is not concave, so that the validity of this inequality does not extend in an obvious way from pure to general (mixed) states.

As shown by Maassen and Uffink [6,15], the Deutsch EUR (4) can be derived from Eq. (7). In the following we will prove that use of the Landau-Pollak inequality (7) actually enables us to obtain a stronger EUR, which improves even on the Maassen-Uffink EUR (6) for pairs of observables such that

$$c(A,B) \geq \frac{1}{\sqrt{2}} \simeq 0.707. \tag{9}$$

As a by-product, our discussion will clarify the conditions under which the Landau-Pollak inequality places stronger restrictions on the probability distributions of A and B than the Maassen-Uffink uncertainty relation.

II. MINIMIZATION OF THE ENTROPY SUM UNDER THE LANDAU-POLLAK CONSTRAINT

We proceed by finding the minimum of the entropy sum $H(A)+H(B)$ with the constraint given by Eq. (7). To achieve this goal, we first consider the minima of the entropy $H(X)$ for probability distributions which have a fixed value P for their maximum probability. That is, we seek for the minimum values of the N-variable function $H(X) = \Sigma_{i=1}^N p_i(X)\ln p_i(X)$ with the constraints $\Sigma_{i=1}^N p_i(X) = 1$ and $\max_i p_i(X) = P$; notice that the maximum probability can be repeated M times, with $1 \leq M \leq N$, so the last constraint is in fact a set of M constraints applying for $i = 1,\ldots,M$. The solution to this problem can be found in Ref. [18], where it is proved that the minimum values of $H(X)$ are attained for the probability distributions of the form

$$\{p_i(X)\}_{\min} = \left\{\underbrace{P,\ldots,P}_{M \text{ times}}, 1-MP, \underbrace{0,\ldots,0}_{N-M-1 \text{ times}}\right\}, \tag{10}$$

the corresponding values of the entropy being then

$$H_{\min}(X) = -MP \ln P - (1-MP)\ln(1-MP), \tag{11}$$

for whatever values of M and P such that

$$M \leq \frac{1}{P} < M+1. \tag{12}$$

The previous result enables us to reduce the problem of finding the minimum of the entropy sum $H(A)+H(B)$ to a simpler one, namely that of minimizing the two-variable functional

$$\begin{aligned}\mathcal{H}(P_A,P_B) &\equiv H_{\min}(A) + H_{\min}(B) \\ &= \sum_{i=A,B} [-M_iP_i \ln P_i - (1-M_iP_i)\ln(1-M_iP_i)]\end{aligned} \tag{13}$$

with the constraints

$$M_i \leq \frac{1}{P_i} < M_i + 1 \quad (M_i \in \mathbb{N}, i = A,B) \tag{14}$$

and Eq. (7). For convenience, we will find instead the maximum of $-\mathcal{H}$, by applying to this functional the (Karush)-Kuhn-Tucker theory for optimization subject to inequality constraints [19].

Let us first exclude the case in which $P_i = 1/M_i$ for at least one i, which will be treated separately. The Lagrangian for this problem is

$$\begin{aligned}\mathcal{L} = \sum_{i=A,B} \Bigg[& M_iP_i \ln P_i + (1-M_iP_i)\ln(1-M_iP_i) \\ & + \mu_i\left(\frac{1}{M_i} - P_i\right) + \nu_i\left(P_i - \frac{1}{M_i+1}\right)\Bigg] \\ & + \lambda(\arccos\sqrt{P_A} + \arccos\sqrt{P_B} - \arccos c),\end{aligned} \tag{15}$$

where $\lambda, \mu_i, \nu_i \geq 0$ are Lagrange undetermined multipliers. The Kuhn-Tucker necessary conditions [19] for a point to be a maximum are then, with $i = A,B$,

$$M_i \ln\frac{P_i}{1-M_iP_i} - \frac{\lambda}{2\sqrt{P_i(1-P_i)}} - \mu_i + \nu_i = 0, \tag{16}$$

$$\mu_i\left(\frac{1}{M_i}-P_i\right)=0, \tag{17}$$

$$\nu_i\left(P_i-\frac{1}{M_i+1}\right)=0, \tag{18}$$

$$\lambda(\arccos\sqrt{P_A}+\arccos\sqrt{P_B}-\arccos c)=0, \tag{19}$$

provided that Eqs. (7) and (14) are still fulfilled. Notice that the Kuhn-Tucker conditions are necessary for a point to be a maximum, but they are not sufficient. Therefore, once we find all the solutions of Eqs. (7), (14), and (16)–(19) we will have to check which one corresponds to the actual maximum.

Since we are restricting ourselves to the case when $P_i \neq 1/M_i$ for $i=A,B$, we must set $\mu_i=\nu_i=0$ also for $i=A,B$ if we want Eqs. (17) and (18) to be compatible with Eq. (14). If $\lambda=0$ as well, then condition (16) reduces to $P_i=1/(1+M_i)$, which contradicts Eq. (14). Therefore $\lambda\neq 0$, so that Eq. (19) reduces to

$$\arccos\sqrt{P_A}+\arccos\sqrt{P_B}=\arccos c. \tag{20}$$

This means that, as it was reasonable to expect, the optimal probability distribution saturates the Landau-Pollak uncertainty relation. Using the trigonometric identity

$$\arccos x+\arccos y=\arccos[xy-\sqrt{(1-x^2)(1-y^2)}], \tag{21}$$

Eq. (20) implies that

$$c=\sqrt{P_AP_B}-\sqrt{(1-P_A)(1-P_B)}\leq\frac{1-\sqrt{(M_A-1)(M_B-1)}}{\sqrt{M_AM_B}}, \tag{22}$$

where the inequality in the right-hand side follows from Eq. (14). Since $c\in(0,1]$, we see from Eq. (22) that

$$\min(M_A,M_B)=1, \quad c\leq\frac{1}{\sqrt{\max(M_A,M_B)}}. \tag{23}$$

On the other hand, Eq. (16) yields

$$\lambda=2M_A\sqrt{P_A(1-P_A)}\,\ln\frac{P_A}{1-M_AP_A}=2M_B\sqrt{P_B(1-P_B)}\,\ln\frac{P_B}{1-M_BP_B}. \tag{24}$$

Equation (24) has several solutions, each of which provides a possible minimum for $\mathcal{H}$. For instance, if we assume that $P_A=P_B$, then Eq. (20) implies that

$$P_A=P_B=\frac{1+c}{2}, \tag{25}$$

while Eq. (14) and the first equation in (23) impose that $M_A=M_B=1$. Therefore, this solution gives the following candidate for the minimum of $\mathcal{H}$:

$$\mathcal{F}(c)\equiv-(1+c)\ln\frac{1+c}{2}-(1-c)\ln\frac{1-c}{2}. \tag{26}$$

If we now assume that $P_A\neq P_B$, we have $M_A=1$, $M_B=M\in\mathbb{N}$ because of Eq. (23). Then the possible minima of $\mathcal{H}$ come from the solutions of the equation

$$\sqrt{P_A(1-P_A)}\,\ln\frac{P_A}{1-P_A}=M\sqrt{P_B(1-P_B)}\,\ln\frac{P_B}{1-MP_B} \tag{27}$$

for $M=1,2,\ldots,$ each of which will be only valid within the range $c\leq 1/\sqrt{M}$ due to the second equation in (23). Unfortunately, Eq. (27) with $P_A\neq P_B$ cannot be solved by analytical means and its solutions must be calculated numerically. If, recalling Eq. (20), we define

$$P_A\equiv\cos^2\alpha, \quad P_B\equiv\cos^2(\theta-\alpha), \quad c\equiv\cos\theta, \tag{28}$$

then Eq. (27) is rewritten as

$$\sin 2\alpha\,\ln\left(\frac{1+\cos 2\alpha}{1-\cos 2\alpha}\right)+M\sin 2(\alpha-\theta)\times\ln\left(\frac{1+\cos 2(\alpha-\theta)}{2[1-M\cos^2(\alpha-\theta)]}\right)=0, \tag{29}$$

where $\alpha\neq\theta/2,\theta/2+\pi/4$ in order to specify $P_A\neq P_B$. We will denote by $\mathcal{H}_M(c)$ the possible minimum of $\mathcal{H}$ obtained by substituting into Eq. (13) the numerical values of $P_i(c)$ corresponding by means of Eq. (28) to the solution $\alpha(\theta)$ of Eq. (29).

Finally, we consider what happens if we allow $P_i=1/M_i$ for $i=A$ and/or $i=B$. Then we get the solution $P_A=1$, $P_B=c^2$, which yields the possible minimum

$$\mathcal{G}(c)\equiv-c^2[1/c^2]\ln c^2-(1-c^2[1/c^2])\ln(1-c^2[1/c^2]), \tag{30}$$

where $[x]$ denotes the integer part of x. There also exist other solutions which turn out to be uninteresting [20].

We now have to select between all the previous solutions the actual minimum of $\mathcal{H}$, which will be our novel lower bound for $H(A)+H(B)$. For $c\geq 1/\sqrt{2}$ we just have three possibilities, namely the analytical bounds $\mathcal{F}(c)$, $\mathcal{G}(c)$, and the numerical bound $\mathcal{H}_1(c)$. These three possible bounds are plotted in Fig. 1 together with the Maassen-Uffink bound (6). From there we readily see that the actual lower bound on the entropy sum equals $\mathcal{F}(c)$ when $c\geq c^*\simeq 0.834$, and $\mathcal{H}_1(c)$ when $1/\sqrt{2}\leq c\leq c^*$. We also see that, in both cases, our lower bound is stronger than the Maassen-Uffink one. It is worth noting that $\mathcal{G}(c)$ is not the actual minimum for any value of c, although it is very close to the numerical bound $\mathcal{H}_1(c)$ and practically overlaps with it within a considerable range.

On the other hand, in the case when $c\leq 1/\sqrt{2}$ the minimum of $\mathcal{H}$ fails to improve on the Maassen-Uffink bound, as can be readily seen from the graph of $\mathcal{H}_1(c)$ displayed in Fig. 1. Nevertheless, since $\mathcal{G}(c)$ interpolates the Maassen-Uffink bound in the only points in which the latter is optimal, i.e., $c=1/\sqrt{n}$ with $n\in\mathbb{N}$ (see Fig. 1), one could think that the

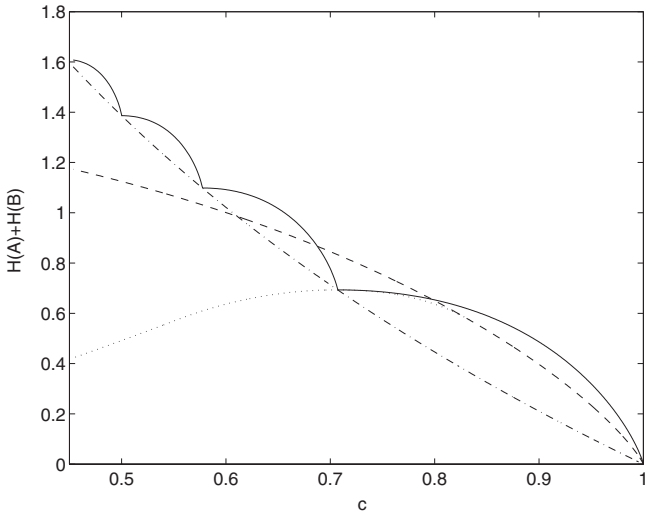

FIG. 1. Actual and possible lower bounds in the EUR (2) for a pair of observables with overlap c: Maassen-Uffink bound (dash-dotted line), $\mathcal{F}(c)$ (dashed line), $\mathcal{H}_1(c)$ (dotted line), and $\mathcal{G}(c)$ (solid line).

former could indeed be the actual lower bound on $H(A)+H(B)$. However, it is possible to find examples with a slightly lower entropy sum that disprove this conjecture.

III. CONCLUSIONS

In summary, using the Landau-Pollak inequality (7) we have managed to improve the Maassen-Uffink bound for EURs in a finite-dimensional Hilbert space for the set of observable pairs that fulfill the large overlap condition (9). The strongest lower bound H_{AB} that is now available for the EUR (2) corresponding to a general pair of observables with overlap c can thus be written as the piecewise function

$$H_{AB}=\begin{cases}-2\ln c & \text{if } 0<c\leq 1/\sqrt{2},\\ \mathcal{H}_1(c) & \text{if } 1/\sqrt{2}\leq c\leq c^*,\\ \mathcal{F}(c) & \text{if } c^*\leq c\leq 1,\end{cases} \tag{31}$$

where $c^*\simeq 0.834$, the analytical bound $\mathcal{F}(c)$ is given by Eq. (26), and the numerical bound $\mathcal{H}_1(c)$ was defined after Eq. (29).

It is interesting to note that for observables acting on a two-dimensional Hilbert space, where the large overlap condition (9) always holds, the bound in Eq. (31) coincides with the optimal bound obtained in [7]. This fact implies that in the general (higher-dimensional) case the bound in Eq. (31) is the best possible bound that can be expressed in terms only of the overlap c. As a by-product, our derivation shows that the Landau-Pollak inequality is optimal in the two-dimensional case.

Our derivation also shows that the Landau-Pollak uncertainty relation is stronger than the Maassen-Uffink EUR for observables that fulfill the large overlap condition (9). It is remarkable that an inequality based on such a simple measure of uncertainty, which ignores all but one of the values of the probability distribution, exhibits this strength. On the other hand, for observables that do not satisfy condition (9), the Landau-Pollak inequality turns out to be weaker than the Maassen-Uffink EUR. As a matter for future research, it would be interesting to check whether other formulations of the uncertainty principle relying on different measures of uncertainty (see Ref. [15]) can be used in an analogous way to derive better bounds for EURs.

ACKNOWLEDGMENTS

We acknowledge support by Dirección General de Investigación (Ministerio de Educación y Ciencia) under Grant No. MTM2006-13000-C03-02 and by Universidad Carlos III de Madrid and Comunidad Autónoma de Madrid (Project No. CCG07-UC3M/ESP-3339). J. S.-R. was also supported by the DGI (MEC) Grant No. FIS2005-00973, and the Junta de Andalucía research group FQM-0207.

[1] H. P. Robertson, Phys. Rev. **34**, 163 (1929).
[2] D. Deutsch, Phys. Rev. Lett. **50**, 631 (1983).
[3] J. B. M. Uffink and J. Hilgevoord, Found. Phys. **15**, 925 (1985); reprinted in *Microphysical Reality and Quantum Description*, edited by F. Selleri, A. van der Merwe, and G. Tarozzi (Reidel, Dordrecht, 1988).
[4] I. Bialynicki-Birula and J. Mycielski, Commun. Math. Phys. **44**, 129 (1975).
[5] K. Kraus, Phys. Rev. D **35**, 3070 (1987).
[6] H. Maassen and J. B. M. Uffink, Phys. Rev. Lett. **60**, 1103 (1988).
[7] A. J. M. Garrett and S. F. Gull, Phys. Lett. A **151**, 453 (1990); J. Sánchez-Ruiz, *ibid.* **244**, 189 (1998).
[8] I. D. Ivanović, J. Phys. A **25**, L363 (1992); J. Sánchez, Phys. Lett. A **173**, 233 (1993); J. Sánchez-Ruiz, J. Phys. A **27**, L843 (1994); Phys. Lett. A **201**, 125 (1995); A. Azarchs, e-print arXiv:quant-ph/0412083v1.
[9] V. Giovannetti, Phys. Rev. A **70**, 012102 (2004); O. Gühne and M. Lewenstein, *ibid.* **70**, 022316 (2004).
[10] D. P. DiVincenzo, M. Horodecki, D. W. Leung, J. A. Smolin, and B. M. Terhal, Phys. Rev. Lett. **92**, 067902 (2004); M. A. Ballester and S. Wehner, Phys. Rev. A **75**, 022319 (2007).
[11] I. B. Damgaard, S. Fehr, R. Renner, L. Salvail, and C. Schaffner, in *Advances in Cryptology—CRYPTO 2007*, edited by A. Menezes, Vol. 4622 of Lecture Notes in Computer Science (Springer, Berlin, 2007), p. 360; J. M. Renes and J.-C. Boileau, e-print arXiv:quant-ph/0702187v1.
[12] C. E. Shannon, Bell Syst. Tech. J. **27**, 379 (1948); **27**, 623 (1948); reprinted in *The Mathematical Theory of Communication*, edited by C. E. Shannon and W. Weaver (University of Illinois Press, Urbana, 1949).
[13] Notice that the concavity of the entropy functional implies that any inequality of the form (2), while stated only for pure states, remains also valid for general (mixed) states. In what

follows, for the sake of brevity, we do not write explicitly the dependence of probability distributions and entropies upon the quantum state of the system.

[14] J. Schwinger, Proc. Natl. Acad. Sci. U.S.A. **46**, 570 (1960); reprinted in *Quantum Kinematics and Dynamics* (Benjamin, New York, 1970).

[15] J. B. M. Uffink, Ph.D. thesis, University of Utrecht, Utrecht, 1990.

[16] H. J. Landau and H. O. Pollak, Bell Syst. Tech. J. **40**, 65 (1961).

[17] J. I. de Vicente and J. Sánchez-Ruiz, Phys. Rev. A **71**, 052325 (2005); T. Miyadera and H. Imai, *ibid.* **76**, 062108 (2007).

[18] M. Feder and N. Merhav, IEEE Trans. Inf. Theory **40**, 259 (1994).

[19] See any standard textbook on optimization, e.g., R. E. Miller, *Optimization, Foundations and Applications* (Wiley-Interscience, New York, 2000).

[20] If only $P_A=1/M_A$, then $\mu_B=\nu_B=0$ and Eqs. (20)–(23) hold like in the previous cases. The analog of Eq. (16) for $i=A$ now imposes that $M_A=1,2$ in order to have non-negativity of the Lagrange multipliers. The solution for $M_A=1$ gives Eq. (30), which is thus proven to be valid in principle for all values of c, while the solution for $M_A=2$ can only hold when $c\leq 1/\sqrt{2}$. If $P_i=1/M_i$ for both A and B, a similar reasoning yields $M_i=1,2$ for $i=A,B$, and the resulting bounds are clearly nonoptimal.