Entropic uncertainty relations for more than two observables

[1]*Contacts: Debbie Leung, wcleung@iqc.ca;*
Stephanie Wehner, wehner@cwi.nl;
Andreas Winter, a.j.winter@bris.ac.uk
(Dated: 4th March 2007)

Background. The uncertainty principle is one of the fundamental ideas of quantum mechanics. Since Heisenberg's uncertainty relations for canonically conjugate variables (formalised by Robertson for arbitrary observables), it has been one of the staples. This, and later, formulations are about the tradeoff between the "uncertainties" in the value of non-commuting observables on the same state preparation; in other words, they are comparing counterfactual situations.

Traditionally, the comparison is between variances of the observables, but it was eventually realised that other measures of "spread" of the distribution on measurement outcomes can be used. Arguably the universal such measure is the entropy of the distribution, and Białynicki-Birula and Mycielski [1] proved an entropic uncertainty relation for systems of n canonical pairs of position and momentum coordinates X_i and P_i:

$$H(X_1 \dots X_n|\varphi) + H(P_1 \dots P_n|\varphi) \geq n \log(e\pi),$$

where $H(Q_1 \dots Q_n|\varphi)$ refers to the (differential) Shannon entropy of the joint distribution of the coordinates $Q_1, \dots Q_n$ when measured on the state φ. In [1] it is shown that this relation implies the Heisenberg uncertainty relation.

After that, following initial work by Deutsch and in response to a conjecture by Karl Kraus, the following inequality was proved by Maassen and Uffink [2] for observables in finite dimension d with eigenbases $\mathcal{B}_j = \{|b_1^j\rangle, \dots, |b_d^j\rangle\}$ ($j = 1, 2$) and an arbitrary state φ:

$$H(\mathcal{B}_1|\varphi) + H(\mathcal{B}_2|\varphi) \geq -\log \max_{x,y} |\langle b_x^1|b_y^2\rangle|^2, \tag{1}$$

where $H(\mathcal{B}_j|\varphi) = H\left(\{|\langle b_x^j|\varphi\rangle|^2 : x = 1, \dots, d\}\right)$ is the Shannon entropy of measuring the state φ in basis $\mathcal{B}_j$. In particular, for mutually unbiased bases, i.e. when all the inner products on the right hand side above are equal to $1/d$, we obtain that the entropy sum is lower bounded by $\log d$. This is tight, as the example of $|\varphi\rangle = |b_x^j\rangle$ shows.

Note that in both cases we get a lower bound on the entropy sum of two non-commuting (and indeed non-coexistent) observables which is independent of the underlying state. This lower bound is not necessarily tight (as can be seen rather easily in the case of the general Maassen-Uffink inequality), but its usefulness lies in the fact that it is in terms of *very simple* geometric information of the relative position of the bases.

The problem. Traditionally, uncertainty relations were restricted to pairs of "conjugate" observables. But the finite-dimensional inequalities, culminating in the Maassen-Uffink one, show that it is really the property of mutual unbiasedness that makes for maximal uncertainty. Since this realisation, one could ask for the entropic uncertainty tradeoff between more than two observables. This may be physically interesting, since there exists in every dimension d a large number of mutually unbiased bases, up to $d + 1$ (see problem 13 on these pages).

In [3] it was shown that for k observables in $\mathbb{C}^d$, with eigenbases $\mathcal{B}_j = \{U_j|x\rangle : x = 1, \dots, d\}$, the expression

$$h(d; U_1, \dots, U_k) := \min_{\varphi} \frac{1}{k} \sum_{j=1}^{k} H(\mathcal{B}_j|\varphi)$$

has information-theoretic significance in the context of "information locking". Here, $H(\mathcal{B}_j|\varphi) = H\left(\{|\langle x|U_j^*|\varphi\rangle|^2 : x = 1, \ldots, d\}\right)$ is the Shannon entropy of the measurement of basis $\mathcal{B}_j$ on the state φ.

Note that always

$$0 \leq h(d; U_1, \ldots, U_k) \leq \left(1 - \frac{1}{k}\right) \log d, \tag{2}$$

and the problem of the entropic uncertainty relations at its most general is to find an expression for or at least a lower bound on $h(d; U_1, \ldots, U_k)$ in "simple" terms of the geometry of the set of bases $\mathcal{B}_j$.

In the applications as the cited one [3], one is interested in maximally unbiased observables, i.e., in

$$h(d; k) := \max_{U_1,\ldots,U_k} h(d; U_1, \ldots, U_k),$$

and a characterisation of the maximisers. Note that if there exist, in dimension d, k mutually unbiased bases, then by virtue of (1) and the above (2),

$$\frac{1}{2} \log d \leq h(d; k) \leq \left(1 - \frac{1}{k}\right) \log d,$$

and one would like to have a characterisation of the sets of unitaries attaining the maximum.

Seeing thus the scaling of $h(d; k)$ with $\log d$, and assuming an asymptotic viewpoint of large dimension, we consider finally the quantity

$$h(k) := \lim_{d\to\infty} \frac{1}{\log d} h(d; k)$$

[if the limit exists, otherwise take the lim inf], which depends now only on k. For example, $h(2) = 1/2$, and it is clear that

$$h(k + k') \geq \frac{k}{k + k'} h(k) + \frac{k'}{k + k'} h(k'),$$

but we don't know if $h(k)$ actually strictly grows with k. If so, does it approach the value $1 - 1/k$ suggested by the upper bound, or at least $1 - 1/f(k)$ with some growing function f of k?

Partial results. In [3] (see the eprint version) numerical work on three and more mutually unbiased bases in dimensions up to 29 is reported, which are consistent with a behaviour of $1 - O(1/k)$ of $h(k)$. The mutually unbiased bases are taken as a subset of the "stabiliser construction" MUBs in prime power dimension.

That this choice may be significant became obvious only with [4] where it was shown that in square prime power dimensions $d = p^{2\ell}$ there exist up to $k = p^\ell + 1$ MUBs with $h(d; U_1, \ldots, U_k) = \frac{1}{2} \log d$ [8]. Furthermore, in any square dimension $d = d_0^2$ a number $k = d^{1/14.8}$ of mutually unbiased bases with the same property can be found. This shows that mutual unbiasedness is not enough to characterise a large $h(d; U_1, \ldots, U_k)$. Indeed, Ambainis [5] has shown that any three bases from the "standard" mutually unbiased bases construction in prime power dimension, $h(d; U_1, U_2, U_3) = \left(\frac{1}{2} + o(1)\right) \log d$, for large dimension, and assuming the Generalised Riemann Hypothesis. Furthermore, for any $0 \leq \epsilon \leq 1/2$, there always exist $k = d^\epsilon$ many of these bases such that $h(d; U_1, \ldots, U_k) = \left(\frac{1}{2} + \epsilon + o(1)\right) \log d$.

On the other hand, it was shown in [6] that $k = (\log d)^4$ unitaries U_j randomly and independently chosen from the Haar measure have $h(d; U_1, \ldots, U_k) \geq \log d - O(1)$ with high probability, and for sufficiently large dimension d.

It should be noted that in the application to information locking, one is interested in a small number of bases; however, for a complete set of mutually unbiased bases in dimension d, Sanchez-Ruiz [7] has shown that $h(d; U_1, \ldots, U_{d+1}) \geq \log(d+1) - 1$.

---

[1] I. Białynicki-Birula, J. Mycielski, "Uncertainty Relations for Information Entropy in Wave Mechanics", Comm. Math. Phys. **44**, 129-132 (1975).

[2] H. Maassen, J. B. M. Uffink, "Generalized Entropic Uncertainty Relations", Phys. Rev. Lett. **60**(12), 1103-1106 (1988).

[3] D. P. DiVincenzo, M. Horodecki, D. W. Leung, J. A. Smolin, B. M. Terhal, "Locking Classical Correlations in Quantum States", Phys. Rev. Lett. **92**(6). 067902 (2004); quant-ph/0303088.

[4] M. A. Ballester, S. Wehner, "Entropic uncertainty relations and locking: tight bounds for mutually unbiased bases", Phys. Rev. A **75**, 022319 (2007); quant-ph/0606244.

[5] A. Ambainis, work to appear (dated October 2006).

[6] P. Hayden, D. W. Leung, P. W. Shor, A. Winter, "Randomizing quantum states: Constructions and applications", Comm. Math. Phys. **250**, 371-391 (2004).

[7] J. Sanchez-Ruiz, "Entropic uncertainty and certainty relations for complementary observables", Phys. Lett. A **173**, 233-239 (1993).

[8] And many more if one relaxes the condition of mutual unbiasedness to approximate unbiasedness, using the techniques of [6].