Universal Uncertainty Relations

Gilad Gour,[1, *] Shmuel Friedland,[2] and Vlad Gheorghiu[1]
[1] *Institute for Quantum Science and Technology and Department of Mathematics and Statistics, University of Calgary, 2500 University Drive NW, Calgary, AB, T2N 1N4, Canada*
[2] *Department of Mathematics, Statistics and Computer Science, University of Illinois at Chicago, 851 S. Morgan Street, Chicago, IL 60607-7045, U.S.A.*

(Dated: Version of June 19, 2013)

Uncertainty relations are a distinctive characteristic of quantum theory that imposes intrinsic limitations on the precision with which physical properties can be simultaneously determined. The modern work on uncertainty relations employs entropic measures to quantify the lack of knowledge associated with measuring non-commuting observables. However, I will show in this talk that there is no fundamental reason for using entropies as quantifiers; in fact, any functional relation that characterizes the uncertainty of the measurement outcomes can be used to define an uncertainty relation. Starting from a simple assumption that any measure of uncertainty is non-decreasing under mere relabeling of the measurement outcomes, I will show that Schur-concave functions are the most general uncertainty quantifiers. I will then introduce a novel fine-grained uncertainty relation written in terms of a majorization relation, which generates an infinite family of distinct scalar uncertainty relations via the application of arbitrary measures of uncertainty. This infinite family of uncertainty relations includes all the known entropic uncertainty relations, but is not limited to them. In this sense, the relation is universally valid and captures the essence of the uncertainty principle in quantum theory.

Uncertainty relations lie at the core of quantum cryptography and are a direct manifestation of the non-commutative structure of quantum mechanics. In contrast to classical physics, where in principle any observable can be measured with arbitrary precision, quantum mechanics introduces severe restrictions on the allowed measurement results of two or more non-commuting observables. Uncertainty relations are not a manifestation of the experimentalists' (in)ability of performing precise measurements, but are inherently determined by the incompatibility of the measured observables.

The first formulation of the uncertainty principle was provided by Heisenberg [1], who noted that more knowledge about the position of a *single* quantum particle implies less certainty about its momentum and vice-versa. He expressed the principle in terms of standard deviations of the momentum and position operators

$$\Delta X \cdot \Delta P \geqslant \frac{\hbar}{2}. \tag{1}$$

Robertson [2] generalized Heisenberg's uncertainty principle to any two arbitrary observables A and B as

$$\Delta A \cdot \Delta B \geqslant \frac{1}{2}|\langle\psi|[A,B]|\psi\rangle|. \tag{2}$$

A major drawback of Robertson's uncertainty principle is that it depends on the state $|\psi\rangle$ of the system. In particular, when $|\psi\rangle$ belongs to the null-space of the commutator $[A,B]$, the right upper bound becomes trivially zero. Deutsch [3] addressed this problem by providing an *entropic* uncertainty relation (EUR) in terms of the Shannon entropies of any two non-degenerate observables, later improved by Maassen and Uffink [4] to

$$H(A) + H(B) \geqslant -2\log c(A,B). \tag{3}$$

Here $H(A)$ is the Shannon entropy [5] of the probability distribution induced by measuring the state $|\psi\rangle$ of the system in the eigenbasis $\{|a_j\rangle\}$ of the oservable A (and similarly for B). The bound on the right hand side $c(A,B) := \max_{m,n}|\langle a_m|b_n\rangle|$ represents the maximum overlap between the bases elements, and is independent of the state $|\psi\rangle$.

Recently the study of uncertainty relations intensified (see [6] for a recent survey), and as a result various important applications have been discovered, ranging from security proofs for quantum cryptography [7–9], information locking [9], non-locality [10], and the separability problem [11]. There were also recent attempts to generalize uncertainty relations to more than two observables. For this case relatively little is known [12–16], as the authors investigated only particular instances of the problem such as mutually unbiased bases.

In most of the recent work on uncertainty relations, entropy functions like the Shannon and Renyi entropies are used to quantify uncertainty. Such entropies are used in information theory to quantify asymptotic rates of certain information processing tasks [5], in which the concepts of typical sets play a crucial role. However, in the context of the uncertainty principle where a single physical system is involved, these entropies are not necessarily the most adequate to use. Indeed, as will be shown in the

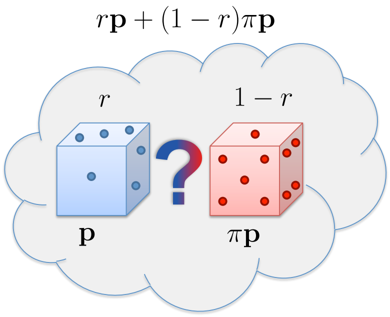

FIG. 1: With probability r Alice samples from a random variable (blue dice), and with probability $1-r$, Alice samples from its relabeling (red dice), but at the end of the protocol she "forgets" where she sampled from. The resulting probability distribution $r\boldsymbol{p}+(1-r)\pi\boldsymbol{p}$ is more uncertain than the initial one associated with the blue (red) dice $\boldsymbol{p}$ ($\pi\boldsymbol{p}$). Color online.

talk, other functions can be more suitable in providing a quantitative description for the uncertainty principle.

Uncertainty is related to the "spread" of a probability distribution, or, equivalently, to the ability of learning that probability distribution. Intuitively a less spread distribution is more certain than a more widely spread. For example, in a d-dimensional sample space, the probability distribution $\boldsymbol{p}=(1,0,\ldots,0)$ is the most certain, whereas the distribution $\boldsymbol{q}=(1/d,1/d,\ldots,1/d)$ is the most uncertain. What are then the minimum requirements that a good measure of uncertainty has to satisfy?

In his seminal paper [3] on EURs, Deutsch pointed out that the standard deviation Δ can be increased by mere relabelling of the random variables associated with the measurements. He therefore concluded that the relation in (1) can not be used as a quantitative description of the uncertainty principle. Following Deutsch observation, we assume in [20] that the uncertainty about a random variable can not increase under a relabelling of its alphabet. We call this very reasonable presumption *monotonicity under relabelling* (MUR). This is our *only* requirement from a measure of uncertainty.

There are several consequences of the MUR assumption. First, the uncertainty associated with a probability vector $\boldsymbol{p}$ can not be larger than the uncertainty associated with a relabelled version of it, $\pi\boldsymbol{p}$, where π is some permutation matrix. In fact, both uncertainties are the same as permutations acting on a probability space are reversible. Second, the uncertainty can not decrease under *random* re-labelings, see Fig. 1. We therefore conclude that any reasonable measure of uncertainty is a function only of the probability vector, is invariant under permutations of its elements, and must be non decreasing under a random relabelling of its argument.

We formulate the above requirements quantitatively using Birkhoff's theorem [17, 18], which states that the convex hull of permutation matrices is the class of doubly-stochastic matrices (their components are non-negative real numbers, and each row and column sums to 1). Birkhoff theorem thus implies that a probability vector $\boldsymbol{q}$ obtained from $\boldsymbol{p}$ by a random relabeling is more uncertain than the latter if and only if the two are related by a doubly-stochastic matrix, $\boldsymbol{q}=D\boldsymbol{p}$, which is equivalent to $\boldsymbol{q}\prec\boldsymbol{p}$. The last equation is known as a majorization relation [19] and consists of a system of d inequalities[1]. The above discussion implies that any measure of uncertainty has to preserve the partial order induced by majorization. The class of functions that preserve this order are the Schur-concave functions. These are functions Φ on a d-dimensional probability space, $\Phi:\mathbb{R}^d\longrightarrow\mathbb{R}$, for which $\Phi(\boldsymbol{x})\geqslant\Phi(\boldsymbol{y})$ whenever $\boldsymbol{x}\prec\boldsymbol{y}$, $\forall\boldsymbol{x},\boldsymbol{y}\in\mathbb{R}^d$. We therefore define a measure of uncertainty as being any non-negative Schur-concave function that takes the value zero on the vector $\boldsymbol{x}=(1,0,\ldots,0)$. The last requirement is not essential but is convenient as it ensures that the measure is non-negative definite.

Our definition for a measure of uncertainty is very general and resulted solely from requiring monotonicity under relabellings; it also encompasses the most common entropy functions used in information theory, but it is not restricted to them. As we are not concerned with asymptotic regimes, we use in the following the most general Φ to quantify uncertainty, without making any assumptions about its functional form.

Having defined what a measure of uncertainty is, we now use it to study uncertainty relations. Let ρ be a mixed state on a d-dimensional Hilbert space $\mathcal{H}\cong\mathbb{C}^d$. For simplicity of the exposition, we first consider two basis (projective) measurements. We denote the two orthonormal bases of $\mathcal{H}$ by $\{|a_m\rangle\}_{m=1}^d$ and $\{|b_n\rangle\}_{n=1}^d$. We also denote by $p_m(\rho)=\langle a_m|\rho|a_m\rangle$ and $q_n(\rho)=\langle b_n|\rho|b_n\rangle$ the two probability distributions obtained by measuring ρ with respect to these bases. We collect the numbers $p_m(\rho)$ and $q_n(\rho)$ into two probability vectors $\boldsymbol{p}(\rho)$ and $\boldsymbol{q}(\rho)$, respectively. The goal of our work is to bound the uncertainty about $\boldsymbol{p}(\rho)$ and $\boldsymbol{q}(\rho)$ by a quantity that depends only on the bases elements but not on the state ρ. The object of our investigation is therefore the joint probability distribution $\boldsymbol{p}(\rho)\otimes\boldsymbol{q}(\rho)$.

The main result in our article [20] is an uncertainty relation of the form

$$\boldsymbol{p}(\rho)\otimes\boldsymbol{q}(\rho)\prec\boldsymbol{\omega},\quad\forall\rho,\tag{4}$$

where $\boldsymbol{\omega}$ is some vector independent of ρ that we explicitly calculate. We call (4) a *universal uncertainty relation*

[1] A vector $\boldsymbol{x}\in\mathbb{R}^d$ *is majorized by* a vector $\boldsymbol{y}\in\mathbb{R}^d$, and write $\boldsymbol{x}\prec\boldsymbol{y}$, whenever $\sum_{j=1}^k x_j^\downarrow\leqslant\sum_{j=1}^k y_j^\downarrow$ for all $1\leqslant k\leqslant d-1$, with $\sum_{j=1}^d x_j^\downarrow=\sum_{j=1}^d y_j^\downarrow$. The down-arrow notation denotes that the component of the corresponding vector are ordered in decreasing order, $x_1^\downarrow\geqslant x_2^\downarrow\geqslant\cdots\geqslant x_d^\downarrow$.

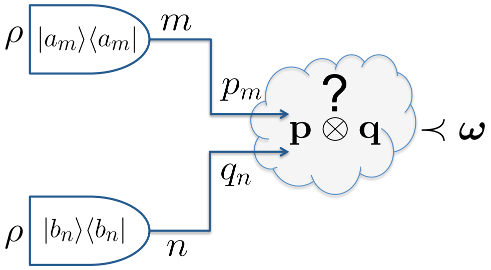
ρ
$|a_m\rangle\langle a_m|$
m
p_m
?
$\mathbf{p} \otimes \mathbf{q}$
$\prec \boldsymbol{\omega}$
q_n
ρ
$|b_n\rangle\langle b_n|$
n

FIG. 2: A quantum state is measured using two orthonormal bases. We collect the induced joint probability distribution in a vector $\boldsymbol{p} \otimes \boldsymbol{q}$ and quantify its uncertainty in terms of a majorization relation, independently of the state ρ. Color online.

(UUR) as, for any measure of uncertainty Φ,

$$\Phi\left(\boldsymbol{p}(\rho) \otimes \boldsymbol{q}(\rho)\right) \geqslant \Phi(\boldsymbol{\omega}), \quad \forall \rho. \tag{5}$$

The UUR (4) generates in fact an infinite family of uncertainty relations of the form (5), one for each Φ. The right hand side of (5) provides a single-number lower bound on the uncertainty of the joint measurement results. Whenever Φ is additive under tensor products (e.g. Renyi entropies), (5) splits as

$$\Phi(\boldsymbol{p}(\rho)) + \Phi(\boldsymbol{q}(\rho)) \geqslant \Phi(\boldsymbol{\omega}). \tag{6}$$

A vector $\boldsymbol{\omega_{op}}$ is *optimal* for the UUR (4) whenever $\boldsymbol{\omega_{op}} \prec \boldsymbol{\omega}$ for all $\boldsymbol{\omega}$ that satisfy (4). In [20] we find out this optimal $\boldsymbol{\omega_{op}}$. Moreover, we generalize the above UUR to the most general setting of $L \geq 2$ POVMs. Our relations are "fine-grained"; they do not depend on a single number (such as the maximum overlap between bases elements), but on *all* components of vector $\boldsymbol{\omega}$, which we compute explicitly, via a majorization relation. Our uncertainty relations are *universal* and capture the essence of uncertainty in quantum mechanics, as they are not quantified by particular measures of uncertainty such as Shannon or Renyi entropies.

In the case of $L > 2$ measurements some uncertainty relations can be trivially generated by a summing pairwise two-measurement uncertainty relations, one for each pair of observables. However, our UURs in [20] are much more powerful and not of this form. This fact can be seen most clearly in a set of measurement operators in which any two observables share a common eigenvector. In this case, a two-measurement uncertainty relation will provide a trivial lower bound of zero (hence the pairwise sum must also be zero) whereas our UUR provides a non-trivial (i.e. non-zero) lower bound.

[*] Electronic address: gour@ucalgary.ca

[1] W. Heisenberg, Zeitschrift für Physik **43**, 172 (1927).
[2] H. P. Robertson, Phys. Rev. **34**, 163 (1929), URL `http://link.aps.org/doi/10.1103/PhysRev.34.163`.
[3] D. Deutsch, Phys. Rev. Lett. **50**, 631 (1983), URL `http://link.aps.org/doi/10.1103/PhysRevLett.50.631`.
[4] H. Maassen and J. B. M. Uffink, Phys. Rev. Lett. **60**, 1103 (1988), URL `http://link.aps.org/doi/10.1103/PhysRevLett.60.1103`.
[5] T. M. Cover and J. A. Thomas, *Elements of Information Theory* (Wiley, New York, 2005), 2nd ed.
[6] S. Wehner and A. Winter, New Journal of Physics **12**, 025009 (2010), URL `http://stacks.iop.org/1367-2630/12/i=2/a=025009`.
[7] I. B. Damgaard, S. Fehr, R. Renner, L. Salvail, and C. Schaffner, in *Advances in Cryptology—CRYPTO '07, Vol. 4622 of Lecture Notes in Computer Science* (Springer, 2007), pp. 360–378.
[8] R. Konig, S. Wehner, and J. Wullschleger, IEEE Trans. Inf. Theory **58**, 1962 (2012), ISSN 0018-9448.
[9] S. Wehner, C. Schaffner, and B. M. Terhal, Phys. Rev. Lett. **100**, 220502 (2008), URL `http://link.aps.org/doi/10.1103/PhysRevLett.100.220502`.
[10] J. Oppenheim and S. Wehner, Science **330**, 1072 (2010), http://www.sciencemag.org/content/330/6007/1072.full.pdf, URL `http://www.sciencemag.org/content/330/6007/1072.abstract`.
[11] O. Gühne, Phys. Rev. Lett. **92**, 117903 (2004), URL `http://link.aps.org/doi/10.1103/PhysRevLett.92.117903`.
[12] I. D. Ivanovic, J. Phys. A: Math. Gen. **25**, L363 (1992), URL `http://stacks.iop.org/0305-4470/25/i=7/a=014`.
[13] J. Sanchez-Ruiz, Physics Letters A **173**, 233 (1993), ISSN 0375-9601, URL `http://www.sciencedirect.com/science/article/pii/0375960193902696`.
[14] M. A. Ballester and S. Wehner, Phys. Rev. A **75**, 022319 (2007), URL `http://link.aps.org/doi/10.1103/PhysRevA.75.022319`.
[15] S. Wu, S. Yu, and K. Mølmer, Phys. Rev. A **79**, 022104 (2009), URL `http://link.aps.org/doi/10.1103/PhysRevA.79.022104`.
[16] S. Wehner and A. Winter, J. Math. Phys. **49**, 062105 (pages 11) (2008), URL `http://link.aip.org/link/?JMP/49/062105/1`.
[17] G. Birkhoff, Univ. Nac. Tucumán. Rev. Ser. A **5**, 147 (1946).
[18] R. Bhatia, *Matrix Analysis* (Springer-Verlag, New York, 1997).
[19] M. Albert W., O. Ingram, and B. C. Arnold, *Inequalities: Theory of Majorization and Its Applications (2nd Edition)*, Springer Series in Statistics (Springer, 2011).
[20] S. Friedland, V. Gheorghiu, G. Gour, *Universal Uncertainty Relations* arXiv:1304.6351.