IOPscience iopscience.iop.org

Home Search Collections Journals About Contact us My IOPscience

Entropic uncertainty relations—a survey

This content has been downloaded from IOPscience. Please scroll down to see the full text.

2010 New J. Phys. 12 025009

(http://iopscience.iop.org/1367-2630/12/2/025009)

View the table of contents for this issue, or go to the journal homepage for more

Download details:

IP Address: 131.180.33.71
This content was downloaded on 17/03/2017 at 12:19

Please note that terms and conditions apply.

You may also be interested in:

R{\eacute}nyi formulation of the entropic uncertainty principle for POVMs
Alexey E Rastegin

Simplified instantaneous non-local quantum computation with applications to position-based cryptography
Salman Beigi and Robert König

About SIC POVMs and discrete Wigner distributions
Samuel Colin, John Corbett, Thomas Durt et al.

Notes on general SIC-POVMs
Alexey E Rastegin

Entanglement in mutually unbiased bases
M Wieniak, T Paterek and A Zeilinger

The link between entropic uncertainty and nonlocality
Marco Tomamichel and Esther Hänggi

On a generalized entropic uncertainty relation in the case of the qubit
S Zozor, G M Bosyk and M Portesi

Entropic formulation of the uncertainty principle for the number and annihilation operators
Alexey E Rastegin

A monogamy-of-entanglement game with applications to device-independent quantum cryptography
Marco Tomamichel, Serge Fehr, Jdrzej Kaniewski et al.

New Journal of Physics
The open-access journal for physics

Entropic uncertainty relations—a survey

Stephanie Wehner[1,3] **and Andreas Winter**[2,3,4]

[1] Institute for Quantum Information, Caltech, Pasadena, CA 91125, USA
[2] Department of Mathematics, University of Bristol, Bristol BS8 1TW, UK
[3] Centre for Quantum Technologies, National University of Singapore, 2 Science Drive 3, Singapore 117542, Singapore
E-mail: wehner@caltech.edu and a.j.winter@bris.ac.uk

New Journal of Physics **12** (2010) 025009 (22pp)
Received 27 July 2009
Published 26 February 2010
Online at http://www.njp.org/
doi:10.1088/1367-2630/12/2/025009

Abstract. Uncertainty relations play a central role in quantum mechanics. Entropic uncertainty relations in particular have gained significant importance within quantum information, providing the foundation for the security of many quantum cryptographic protocols. Yet, little is known about entropic uncertainty relations with more than two measurement settings. In the present survey, we review known results and open questions.

[4] Authors to whom any correspondence should be addressed.

© IOP Publishing Ltd and Deutsche Physikalische Gesellschaft

Contents

The uncertainty principle is one of the fundamental ideas of quantum mechanics. Since Heisenberg's uncertainty relations for canonically conjugate variables, they have been one of the most prominent examples of how quantum mechanics differs from the classical world (Heisenberg 1927). Uncertainty relations today are probably best known in the form given by Robertson (1929), who extended Heisenberg's result to two arbitrary observables A and B. Robertson's relation states that if we prepare many copies of the state $|\psi\rangle$, and measure each copy individually using either A or B, we have

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

where $\Delta X = \sqrt{\langle\psi|X^2|\psi\rangle - \langle\psi|X|\psi\rangle^2}$ for $X \in \{A, B\}$ is the standard deviation resulting from measuring $|\psi\rangle$ with observable X. The consequence is the complementarity of quantum mechanics: there is no way to simultaneously specify definite values of non-commuting observables. This, and later, formulations concern themselves with 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.

It was eventually realized that other measures of 'spread' of the distribution on measurement outcomes can be used to capture the essence of uncertainty relations, which can be advantageous. Arguably the universal measure is the entropy of the distribution, which led Hirschmann to propose the first entropic uncertainty relation for position and momentum observables (Hirschmann 1957). His results were later improved by the inequalities of Beckner (1975) and the uncertainty relations of Białynicki-Birula and Mycielski (1975), which we will review below. In Białynicki-Birula and Mycielski (1975) it is shown that this relation implies the Heisenberg uncertainty relation (1), and thus entropic uncertainty relations provide us with a more general framework of quantifying 'uncertainty'.

That entropic uncertainty relations are indeed desirable was pointed out by Deutsch (1983), who emphasized the fact that the lower bound given by Robertson's uncertainty relation depends on the state $|\psi\rangle$. In particular, this lower bound is trivial when $|\psi\rangle$ happens to give zero expectation on $[A, B]$—which in finite dimension is always possible. He addressed this problem by proving a first entropic uncertainty relation in terms of the Shannon entropy for *any* two non-degenerate observables, which gives a bound that is *independent* of the state to be measured. His uncertainty relation was later improved by Maassen and Uffink (1988), following a conjecture by Kraus (1987), which we will discuss in detail below. Apart from placing universal lower bounds on uncertainty even in finite dimension, another side effect of considering entropy uncertainty relations is a conceptual liberation. Indeed, Robertson's inequality (1) is best when the right hand side is $\mathbb{1}$, i.e. A and B are canonically conjugate which happens if and only if they are related by a Fourier transform. In the finite-dimensional case, Maassen and Uffink (1988) show that the largest uncertainty is obtained more generally for so-called *mutually unbiased* observables, which opens the way for uncertainty tradeoffs of more than two observables. Even though entropic uncertainty relations thus play an important role in our understanding of quantum mechanics, and have interesting applications ranging from quantum cryptography (Damgaard *et al* 2005, Koashi 2005), information locking (DiVincenzo *et al* 2004), atomic systems (Srikanth and Banerjee 2009), to the question of separability (Guehne 2004), very little is known about them. Indeed, only in the case of two measurement settings do we have a reasonable understanding of such relations. The purpose of this review is to present what is known about entropic uncertainty relations for a number of different entropic quantities, where we focus on Shannon and Rényi entropies. Other relations are known for a wide range of entropic quantities such as the Fisher information (Gibilisco *et al* 2009), the Tsallis entropy (Majernik and Majernikova 2001, Rajagopal 1995, Tsallis 1988) and other entropies with special properties (Hall 2008). A general survey on uncertainty relations predating most of the results mentioned here can be found in Dodonov and Man'ko (1989).

Let us first consider the general form of an entropic uncertainty relation more formally. Let $\mathcal{M}_j = \{M_j^x \mid M_j^x \in \mathcal{B}(\mathcal{H})\}$ be a measurement on the space $\mathcal{H}$ with a (finite) set of outcomes $x \in \mathcal{X}$, that is, for all x we have $M_j^x \geqslant 0$ and $\sum_x M_j^x = \mathbb{1}$. For any quantum state ρ, the measurement $\mathcal{M}_j$ induces a distribution P_j over the outcomes given by $P_j(x) = \mathrm{Tr}(M_j^x \rho)$. We will write $H_\alpha(\mathcal{M}_j|\rho)$ for an entropy H_α of the resulting distribution. For example, for the Shannon entropy we have

$$H(\mathcal{M}_j|\rho) = -\sum_x \mathrm{Tr}(M_j^x \rho) \log \mathrm{Tr}(M_j^x \rho).$$

An entropic uncertainty relation captures the incompatibility of several measurements $\mathcal{M}_1, \ldots, \mathcal{M}_L$. In particular, any such relation takes the form

$$\text{for all } \rho \in \mathcal{S}(\mathcal{H}) \qquad \frac{1}{L}\sum_{j=1}^{L} H_\alpha(\mathcal{M}_j|\rho) \geqslant c_{\{\mathcal{M}_j\}}, \tag{2}$$

where $c_{\{\mathcal{M}_j\}}$ is a constant depending solely on our choice of measurements, and not on the state ρ. It is a particularly interesting question to find measurements for which $c_{\{\mathcal{M}_j\}}$ is as large as possible.

In section 1, we first provide an overview of the entropic quantities we will use throughout this text. We also introduce the concept of maximally strong uncertainty relations and discuss

mutually unbiased bases, which play a special role in the study of uncertainty relations. We then consider the case of two measurement settings ($L = 2$) in section 2 which is the only case well understood. In section 3, we then present an overview of the few results known for multiple measurements. We conclude in section 4 with some applications of uncertainty relations in cryptography.

1. Preliminaries

1.1. Entropic quantities

We begin by introducing all entropic quantities used in this text. The expert reader may safely skip this section. Let P_X be a distribution over a set $\mathcal{X}$, where we write $P_X(x)$ for the probability of choosing a particular element $x \in \mathcal{X}$. The *Rényi entropy* (Rényi 1960) of this distribution is defined as

$$H_\alpha(P_X) = \frac{1}{1-\alpha} \log \left(\sum_{x \in \mathcal{X}} P_X(x)^\alpha \right),$$

for any $\alpha \geqslant 0$. It will be useful to note that the Rényi entropy is in fact related to the α-norm of the vector v of probabilities

$$\|v\|_\alpha = \left(\sum_{x \in \mathcal{X}} P_X(x)^\alpha \right)^{1/\alpha}$$

by taking the logarithm

$$H_\alpha(P_X) = \frac{\alpha}{1-\alpha} \log \|v\|_\alpha.$$

A special case of the Rényi entropy is the well-known Shannon entropy (Shannon 1948) obtained by taking the limit

$$H(P_X) = \lim_{\alpha \to 1} H_\alpha(P_X) = -\sum_{x \in \mathcal{X}} P_X(x) \log P_X(x).$$

We are especially interested in the so-called *collision entropy*, that is, the Rényi entropy of order $\alpha = 2$ given by

$$H_2(P_X) = -\log \sum_{x \in \mathcal{X}} P_X(x)^2,$$

and the *min-entropy* given by the limit $\alpha \to \infty$ as

$$H_\infty(P_X) = -\log \max_{x \in \mathcal{X}} P_X(x).$$

The Rényi entropies are monotonically decreasing in α, i.e.

$$H_\alpha(\cdot) \geqslant H_\beta(\cdot),$$

for $\alpha \leqslant \beta$. In particular, we thus have $H_\infty(\cdot) \leqslant H_2(\cdot) \leqslant H(\cdot)$. Note that any such entropies can take on values in the interval $0 \leqslant H_\alpha(\cdot) \leqslant \log |\mathcal{X}|$, where the lower bound is clearly attained

if the distribution is sharply defined with $P_X(x) = 1$ for some $x \in \mathcal{X}$, and the upper bound is attained when $P_X(x) = 1/|\mathcal{X}|$ is the uniform distribution.

In the following, we will write

$$H_\alpha(\mathcal{B}|\rho) := H_\alpha(\{|x\rangle\langle x|\}|\rho)$$

to denote the entropy arising from a measurement in an orthonormal basis $\mathcal{B} = \{|x\rangle \mid x \in [d]\}$ where $[d] := \{1, \ldots, d\}$ and use

$$H_\alpha(\mathcal{A}|\rho) := H_\alpha(\{A_x\}|\rho)$$

to denote the entropy arising from measuring with observables $\mathcal{A}$ given by the projectors $\{A_x\}$.

1.2. Maximally strong uncertainty relations

An intriguing question is to find measurements which are very incompatible, in the sense that the rhs of (2) is very large. We will refer to this as a *strong uncertainty relation*. Note that given any set of projective measurements $\mathcal{M}_1, \ldots, \mathcal{M}_L$, we can always find a state ρ such that

$$H_\alpha(\mathcal{M}_j|\rho) = 0$$

for one of the measurements $\mathcal{M}_j$, namely by choosing ρ to be an eigenstate of one of the measurement operators. We thus know that the rhs of (2) can never exceed

$$\log|\mathcal{X}|(1 - 1/L) \geqslant c_{\{\mathcal{M}_j\}} \geqslant 0.$$

If for any choice of measurements the lower bound is given by $c_{\{\mathcal{M}_j\}} = \log|\mathcal{X}|(1 - 1/L)$, we know that if ρ has zero entropy for one of the measurements, the entropy is maximal for all others. We call a set of measurements that satisfy this property *maximally incompatible*, and refer to the corresponding uncertainty relation as being *maximally strong*. Below, we will define a special relationship between two bases called *mutually unbiased*. Such pairs of bases have the property that when we measure any vector from the first basis in the second basis, the outcome over measurement outcomes will be uniform. Indeed, when we consider measurements in L different bases, all bases must be mutually unbiased to each other in order for us to obtain strong uncertainty relations: suppose that two of the L bases $\mathcal{B}_1$ and $\mathcal{B}_2$ are not mutually unbiased, so there exist two basis vectors $|x\rangle \in \mathcal{B}_1$ and $|y\rangle \in \mathcal{B}_2$ that have higher overlap $|\langle x|y\rangle|^2 > 1/d$. Then choosing $\rho = |x\rangle\langle x|$ to be a projector onto a vector of the first basis yields zero entropy when measured in basis $\mathcal{B}_1$ and less than full entropy when measured in the basis $\mathcal{B}_2$. As outlined below, mutually unbiased bases do indeed lead to maximally strong uncertainty relations for $L = 2$ measurements. This however does not hold in general for the case of $L > 2$. We will also see that maximally incompatible measurements can be found for any L if we only consider $|\mathcal{X}| = 2$ outcomes.

1.3. Mutually unbiased bases

Since mutually unbiased bases play an important role in the study of uncertainty relations, we briefly review two well-known constructions for which particular uncertainty relations are known to hold.

1	2	3
2	3	1
3	1	2

1	2	3
3	1	2
2	3	1

Figure 1. Mutually orthogonal Latin squares.

Definition 1.1 (MUBs). *Let* $\mathcal{B}_1 = \{|b_1^1\rangle, \ldots, |b_d^1\rangle\}$ *and* $\mathcal{B}_2 = \{|b_1^2\rangle, \ldots, |b_d^2\rangle\}$ *be two orthonormal bases in* $\mathbb{C}^d$. *They are said to be mutually unbiased if* $|\langle b_k^1|b_l^2\rangle| = 1/\sqrt{d}$, *for every* $k, l \in [d]$ *A set* $\{\mathcal{B}_1, \ldots, \mathcal{B}_m\}$ *of orthonormal bases in* $\mathbb{C}^d$ *is called a* set of mutually unbiased bases *if each pair of bases is mutually unbiased.*

For example, the well-known computational and Hadamard basis are mutually unbiased. We use $N(d)$ to denote the maximal number of MUBs in dimension d. In any dimension d, we have that $\mathrm{N}(d) \leqslant d+1$ (Bandyopadhyay *et al* 2002). If $d = p^k$ is a prime power, we have that $\mathrm{N}(d) = d+1$ and explicit constructions are known (Bandyopadhyay *et al* 2002, Wootters and Fields 1989). If $d = s^2$ is a square, $\mathrm{N}(d) \geqslant \mathrm{MOLS}(s)$ where $\mathrm{MOLS}(s)$ denotes the number of mutually orthogonal $s \times s$ Latin squares (Wocjan and Beth 2005). In general, we have $\mathrm{N}(nm) \geqslant \min\{\mathrm{N}(n), \mathrm{N}(m)\}$ for all $n, m \in \mathbb{N}$ (Klappenecker and Rötteler 2004, Zauner 1999). From this it follows that in any dimension, there is an explicit construction for 3 MUBs (Grassl 2004). Unfortunately, not much else is known. For example, it is still an open problem whether there exists a set of 7 (or even 4!) MUBs in dimension $d = 6$. In this text, we refer to two specific constructions of mutually unbiased bases. There exists a third construction based on Galois rings (Klappenecker and Rötteler 2004), which we do not consider here, since we do not know of any specific uncertainty relations in this setting.

1.3.1. Latin squares. First, we consider MUBs based on mutually orthogonal Latin squares (Wocjan and Beth 2005) which can be constructed in square dimensions $d = s^2$ with $s \in \mathbb{N}$. Informally, an $s \times s$ Latin square over the symbol set $[s]$ is an arrangement of elements of $[s]$ into an $s \times s$ square such that in each row and each column every element occurs exactly once. Let L_{ij} denote the entry in a Latin square in row i and column j. Two Latin squares L and L' are called mutually orthogonal if and only if $\{(L_{i,j}, L'_{i,j})|i, j \in [s]\} = \{(u, v)|u, v \in [s]\}$. Intuitively, this means that if we place one square on top of the other, and look at all pairs generated by the overlaying elements, all possible pairs occur. An example is given in figure 1 below. From any $s \times s$ Latin square we can obtain a basis for $\mathbb{C}^s \otimes \mathbb{C}^s$. Firstly, we construct s of the basis vectors from the entries of the Latin square itself. Let

$$|v_{1,\ell}\rangle = \frac{1}{\sqrt{s}} \sum_{i,j \in [s]} E^L_{i,j}(\ell)|i, j\rangle,$$

where E^L is a predicate such that $E^L_{i,j}(\ell) = 1$ if and only if $L_{i,j} = \ell$. Note that for each ℓ we have exactly s pairs i, j such that $E_{i,j}(\ell) = 1$, because each element of $[s]$ occurs exactly s times in the Latin square. Secondly, from each such vector we obtain $s-1$ additional vectors by adding successive rows of an $s \times s$ complex Hadamard matrix $H = (h_{ij})$ as coefficients to

obtain the remaining $|v_{t,j}\rangle$ for $t \in [s]$, where $h_{ij} = \omega^{ij}$ with $i, j \in \{0, \ldots, s-1\}$ and $\omega = \mathrm{e}^{2\pi \mathrm{i}/s}$. Two additional MUBs can then be obtained in the same way from the two non-Latin squares where each element occurs for an entire row or column, respectively. From each mutually orthogonal Latin square and these two extra squares which also satisfy the above orthogonality condition, we obtain one basis. This construction therefore gives MOLS$(s)+2$ many MUBs, where MOLS(s) is the number of $s \times s$ mutually orthogonal Latin squares. It is known that if $s = p^k$ is a prime power itself, we obtain $p^k + 1 \approx \sqrt{d}$ MUBs from this construction. Note, however, that there do exist many more MUBs in prime power dimensions, namely $d+1$. If s is not a prime power, it is merely known that MOLS$(s) \geqslant s^{1/14.8}$ (Wocjan and Beth 2005).

As an example, consider the first 3×3 Latin square depicted in figure 1 and the 3×3 complex Hadamard matrix

$$H = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix},$$

where $\omega = \mathrm{e}^{2\pi \mathrm{i}/3}$. First, we obtain vectors

$$|v_{1,1}\rangle = \frac{1}{\sqrt{3}}(|1,1\rangle + |2,3\rangle + |3,2\rangle),$$

$$|v_{1,2}\rangle = \frac{1}{\sqrt{3}}(|1,2\rangle + |2,1\rangle + |3,3\rangle),$$

$$|v_{1,3}\rangle = \frac{1}{\sqrt{3}}(|1,3\rangle + |2,2\rangle + |3,1\rangle).$$

With the help of H we obtain three additional vectors from the ones above. From the vector $|v_{1,1}\rangle$, for example, we obtain

$$|v_{1,1}\rangle = \frac{1}{\sqrt{3}}(|1,1\rangle + |2,3\rangle + |3,2\rangle),$$

$$|v_{2,1}\rangle = \frac{1}{\sqrt{3}}(|1,1\rangle + \omega|2,3\rangle + \omega^2|3,2\rangle),$$

$$|v_{3,1}\rangle = \frac{1}{\sqrt{3}}(|1,1\rangle + \omega^2|2,3\rangle + \omega|3,2\rangle).$$

This gives us basis $\mathcal{B} = \{|v_{t,\ell}\rangle | t, \ell \in [s]\}$ for $s = 3$. The construction of another basis follows in exactly the same way from a mutually orthogonal Latin square. The fact that two such squares L and L' are mutually orthogonal ensures that the resulting bases will be mutually unbiased. Suppose we are given another such basis, $\mathcal{B}' = \{|u_{t,\ell}\rangle | t, \ell \in [s]\}$ belonging to L'. We then have for any $\ell, \ell' \in [s]$ that $|\langle u_{1,\ell'}|v_{1,\ell}\rangle|^2 = |(1/s)\sum_{i,j\in[s]} E^{L'}_{i,j}(\ell')E^{L}_{i,j}(\ell)|^2 = 1/s^2$, as there exists exactly only one pair $\ell, \ell' \in [s]$ such that $E^{L'}_{i,j}(\ell')E^{L}_{i,j}(\ell) = 1$. Clearly, the same argument holds for the additional vectors derived from the complex Hadamard matrix.

1.3.2. Generalized Pauli matrices. The second construction we consider is based on the generalized Pauli matrices X_d and Z_d (Bandyopadhyay *et al* 2002), defined by their actions on the computational basis $C = \{|0\rangle, \ldots, |d-1\rangle\}$ as follows:

$$X_d|k\rangle = |k+1 \bmod d\rangle,$$

$$Z_d|k\rangle = \omega^k|k\rangle, \quad \forall\ |k\rangle \in C,$$

where $\omega = \mathrm{e}^{2\pi \mathrm{i}/d}$. We say that $(X_d)^{a_1}(Z_d)^{b_1} \otimes \cdots \otimes (X_d)^{a_N}(Z_d)^{b_N}$ for $a_k, b_k \in \{0, \ldots, d-1\}$ and $k \in [N]$ is a *string of Pauli matrices*. Note that for $d = 2$ these are just the usual Pauli matrices.

If d is a prime, it is known that the $d+1$ MUBs constructed first by Wootters and Fields (Wootters and Fields 1989) can also be obtained as the eigenvectors of the matrices $Z_d, X_d, X_dZ_d, X_dZ_d^2, \ldots, X_dZ_d^{d-1}$ (Bandyopadhyay *et al* 2002). If $d = p^k$ is a prime power, consider all d^2-1 possible strings of Pauli matrices excluding the identity and group them into sets $C_1, \ldots, C_{d+1}$ such that $|C_i| = d-1$ and $C_i \cap C_j = \emptyset$ for $i \neq j$ and all elements of C_i commute. Let B_i be the common eigenbasis of all elements of C_i. Then $B_1, \ldots, B_{d+1}$ are MUBs (Bandyopadhyay *et al* 2002). A similar result for $d = 2^k$ has also been shown in Lawrence *et al* (2002). A special case of this construction are the three mutually unbiased bases in dimension $d = 2^k$ given by the unitaries $\mathbb{1}^{\otimes k}$, $H^{\otimes k}$ and $K^{\otimes k}$ applied to the computational basis, where H is the Hadamard transform and $K = (\mathbb{1} + i\sigma_x)/\sqrt{2}$. A simple example of this construction are the mutually unbiased bases in dimension $d = 2$, which are given by the eigenvectors of the Pauli matrices X, Z and Y. A very interesting aspect of such mutually unbiased bases is that there exists an ordering $\mathcal{B}_1, \ldots, \mathcal{B}_{d+1}$ and a unitary U that cyclically permutes all bases, that is, $U\mathcal{B}_j = \mathcal{B}_{j+1}$ for all j, where $U\mathcal{B}_{d+1} = \mathcal{B}_1$ (Wootters and Sussman 2007).

2. Two measurements

The case of two measurements ($L = 2$) is reasonably well understood in any dimension, and for any number of outcomes. This case was of particular interest as is directly inspired by the two measurements for which Heisenberg had originally formulated his uncertainty relation, i.e. position and momentum. We begin by recalling some of the history of this fascinating problem, before reviewing the currently relevant results.

2.1. History

The first entropic uncertainty relation was given by Hirschmann (1957) for position and momentum observables, which was improved by the inequalities of Beckner (1975) and the entropic uncertainty relations of Białynicki-Birula and Mycielski (1975) to an entropic uncertainty relation for systems of n canonical pairs of position and momentum coordinates X_i and P_i:

$$H(X_1 \ldots X_n|\rho) + H(P_1 \ldots P_n|\rho) \geqslant n \log(e\pi)$$

where $H(Q_1 \ldots Q_n|\varphi)$ refers to the (differential) Shannon entropy of the joint distribution of the coordinates $Q_1, \ldots, Q_n$ when measured on the state ρ. Recall that the differential entropy

of a probability density p (with respect to Lebesgue measure) on $\mathbb{R}^n$ is defined as

$$H(p) = -\int \mathrm{d}x p(x) \log p(x),$$

see Cover and Thomas (1991).

That entropic uncertainty relations are of great importance also in finite dimension was pointed out by Deutsch (1983), who proved that for measurements in two bases $\mathcal{A}$ and $\mathcal{B}$ we have

$$\frac{1}{2}(H(\mathcal{A}|\rho) + H(\mathcal{B}|\rho)) \geqslant -\log\left(\frac{1+c(\mathcal{A},\mathcal{B})}{2}\right),$$

where $c(\mathcal{A},\mathcal{B}) := \max\{|\langle a|b\rangle| \mid |a\rangle \in \mathcal{A}, |b\rangle \in \mathcal{B}\}$. We will see later that the same bound holds for the min-entropies $H_\infty(\cdot)$. His results were extended to a continuous setting for angle–angular momentum and position and momentum by Partovi (1983), which in turn was improved by Białynicki-Birula (1984). Different relations for particular angular momentum observables were later also derived by Białynicki-Birula and Madajczyk (1985). A Rényi entropic version of such an uncertainty relation may be found in Białynicki-Birula (2006).

2.2. *Measurements in different bases*

2.2.1. Any choice of bases. Following a conjecture by Kraus (1987), Maassen and Uffink (1988) improved Deutsch's uncertainty relation for measurements in two different bases. In particular, they showed that if we measure any state $\rho \in \mathcal{H}$ with $\dim \mathcal{H} = d$ using observables with orthonormal eigenbases $\mathcal{A} = \{|a_1\rangle, \ldots, |a_d\rangle\}$ and $\mathcal{B} = \{|b_1\rangle, \ldots, |b_d\rangle\}$, respectively, we have

$$\tfrac{1}{2}(H(\mathcal{A}||\psi\rangle) + H(\mathcal{B}||\psi\rangle)) \geqslant -\log c(\mathcal{A},\mathcal{B}), \tag{3}$$

where $c(\mathcal{A},\mathcal{B}) := \max\{|\langle a|b\rangle| \mid |a\rangle \in \mathcal{A}, |b\rangle \in \mathcal{B}\}$. Since $H(\cdot)$ is concave in $|\psi\rangle$, this result also applies to mixed states ρ. What is the strongest possible relation we could obtain? That is, which choices of $\mathcal{A}$ and $\mathcal{B}$ maximize the rhs of equation (3)? It turns out that the maximum is reached when the two bases are mutually unbiased (see section 1.3), i.e. when all the inner products on the rhs above are equal to $1/\sqrt{d}$. We then obtain that the entropy sum is lower bounded by $\frac{1}{2}\log d$. This is tight, as the example of $|\varphi\rangle = |a_1\rangle$ shows. Note that for general observables, this lower bound is not necessarily tight, but its usefulness lies in the fact that it is in terms of *very simple* geometric information of the relative position of the bases.

2.2.2. Improved bounds for specific bases. For dimension $d = 2$ optimal uncertainty relations have been obtained for two observables $A = \vec{a}\cdot\vec{\sigma}$ and $B = \vec{b}\cdot\vec{\sigma}$ where $\vec{\sigma} = (X, Y, Z)$, for some angles of the Bloch vectors $\vec{a}\cdot\vec{b}$ analytically, and for others numerically (Ghirardi *et al* 2003). Uncertainty relations that give improved bounds for a large class of measurements in two different bases $\mathcal{A}$ and $\mathcal{B}$ have also been obtained in de Vicente and Sanchez-Ruiz (2008) for the case that the overlap between two basis vectors is large, that is, $c(\mathcal{A},\mathcal{B}) \geqslant 1/\sqrt{2}$. Letting $c := c(\mathcal{A},\mathcal{B})$, the following analytical bound is shown for this regime:

$$\frac{1}{2}(H(\mathcal{A}|\rho)H(\mathcal{B}|\rho)) \geqslant -\frac{1+c}{2}\log\left(\frac{1+c}{2}\right) - \frac{1-c}{2}\log\left(\frac{1-c}{2}\right),$$

and a numerical bound is provided that is slightly better for $1/\sqrt{2} \leqslant c \leqslant 0.834$.

2.2.3. Relations for Rényi entropies. It is an often overlooked fact that Maassen and Uffink also show uncertainty relations in terms of the Rényi entropies. In particular, they extend a result by Landau and Pollack (1961) to show that for any $|\psi\rangle$

$$\frac{1}{2}(H_\infty(\mathcal{A}||\psi\rangle) + H_\infty(\mathcal{B}||\psi\rangle)) \geqslant -\log\left[\frac{1+c(\mathcal{A},\mathcal{B})}{2}\right].$$

To see that this bound can be tight for some choices of $\mathcal{A}$ and $\mathcal{B}$, consider two mutually unbiased bases in dimension $d = 2$. For example, the computational $\mathcal{A} = \{|0\rangle, |1\rangle\}$ and the Hadamard basis $\mathcal{B} = \{|+\rangle, |-\rangle\}$. The lower bound then becomes $-\log(1/2 + 1/(2\sqrt{2}))$, which is attained for $|\psi\rangle = \cos(\pi/8)|0\rangle + \sin(\pi/8)|1\rangle$. Furthermore they use a result for α-norms (Riesz 1929) to show that the following relation holds in terms for Rényi entropies of order α and β satisfying $\alpha > 1$ and $\beta = \alpha/(2\alpha - 1) < 1$

$$\tfrac{1}{2}(H_\alpha(\mathcal{A}||\psi\rangle) + H_\beta(\mathcal{B}||\psi\rangle)) \geqslant -\log c(\mathcal{A},\mathcal{B}),$$

for any state $|\psi\rangle$, which gave the result for the Shannon entropy above in the limit of $\alpha, \beta \to 1$. Another uncertainty relation is known for the min-entropy, which has specific cryptographic applications which we will investigate in section 4.

2.3. General measurements

2.3.1. Shannon entropy. The result by Maassen and Uffink (1988) has been extended to the case of a general POVM. The first such result was given by Hall (1997), who pointed out that their result can be easily extended to the case of rank one POVMs. His result was subsequently strengthened (Massar 2007, Rastegin 2008a) by noting that any two POVMS $\mathcal{M}_1 = \{|x_1\rangle\langle x_1| \mid |x_1\rangle \in \mathcal{H}\}$ and $\mathcal{M}_2 = \{|x_2\rangle\langle x_2| \mid |x_2\rangle \in \mathcal{H}\}$ acting on the Hilbert space $\mathcal{H}$ have a Naimark extension to an ancillary space $\mathcal{H}_{\text{anc}}$ such that $U|\tilde{x}_1\rangle = |x_1\rangle + U|\tilde{x}_1\rangle$, and $U|\tilde{x}_2\rangle = |x_2\rangle + U|\hat{x}_2\rangle$ for any unitary $U = (\mathbb{1}_{\mathcal{H}} \oplus V_{\text{anc}})$ acting only on $\mathcal{H}_{\text{anc}}$, where $\{|\hat{x}_1\rangle, |\hat{x}_2\rangle \in \mathcal{H}_{\text{anc}}\}$ form an orthonormal bases on the ancillary system. Maximizing over such unitaries, that is, possible extensions of the POVM, one obtains the bound

$$\tfrac{1}{2}(H(\mathcal{M}_1|\rho) + H(\mathcal{M}_2|\rho)) \geqslant \max_U -\log\max_{x,y} |\langle\tilde{x}_1|U|\tilde{y}_2\rangle|$$

any state $\rho \in \mathcal{B}(\mathcal{H})$. The general setting was analyzed by Krishna and Parthasarathy (2002) who showed that

$$\tfrac{1}{2}(H(\mathcal{M}_1|\rho) + H(\mathcal{M}_2|\rho)) \geqslant -\log\max_{x,y} ||(M_1^{(x)})^{1/2}(M_2^{(y)})^{1/2}||_\infty$$

for any POVMS $\mathcal{M}_1 = \{M_1^{(x)} \mid M_1^{(x)} \in \mathcal{B}(\mathcal{H})\}$ and $\mathcal{M}_2 = \{M_2^{(y)} \mid M_2^{(y)} \in \mathcal{B}(\mathcal{H})\}$ and any state $\rho \in \mathcal{B}(\mathcal{H})$.

2.3.2. Rényi entropy. Entropic uncertainty relations for Rényi entropies have also been obtained for the case of POVMs; however, such bounds depend on the state and thus differ in spirit from the other uncertainty relations we consider. In particular, it has been shown by Rastegin (2008b, c) that for any two POVMS $\mathcal{M}_1$ and $\mathcal{M}_2$ and any state

$$\rho = \sum_j \lambda_j |\psi_j\rangle\langle\psi_j|,$$

we have

$$\frac{1}{2}(H_\alpha(\mathcal{M}_1|\rho) + H_\beta(\mathcal{M}_2|\rho)) \geqslant -\log\left[\max_{j,x,y} \frac{|\langle\psi_j|M_1^{(x)}M_2^{(y)}|\psi_j\rangle|}{||(M_1^{(x)})^{1/2}|\psi_j\rangle||_2||(M_2^{(y)})^{1/2}|\psi_j\rangle||_2}\right],$$

for $1/\alpha + 1/\beta = 2$.

2.4. Quantum side information

In the context of quantum information theoretical applications some other uncertainty relations were discovered, which are entropic in spirit, but lie outside of the formalism introduced above.

Here, we quote two that can be viewed as extensions of the inequality of Maassen and Uffink (1988) in the case of two measurement bases related by the Fourier transform, to multipartite quantum systems and involving the von Neumann entropy $S(\rho) = -\mathrm{Tr}\,\rho\log\rho$. With this entropy, one can formally construct a mutual information and a conditional entropy, respectively, for bipartite states ρ_{AB} with marginals $\rho_A = \mathrm{Tr}_B\rho_{AB}$ and $\rho_B = \mathrm{Tr}_A\rho_{AB}$:

$$I(A:B) = I(A:B)_\rho := S(\rho_A) + S(\rho_B) - S(\rho_{AB}),$$

$$S(A|B) \;= S(A|B)_\rho := S(\rho_{AB}) - S(\rho_B).$$

Both inequalities compare two conjugate bases, i.e. without loss of generality, one is the standard basis $\{|z\rangle : z = 0,\ldots,d-1\}$, the other one its Fourier transform $\left\{|\hat{x}\rangle = \sum_z \mathrm{e}^{2\pi\mathrm{i}xz/d}|z\rangle : x = 0,\ldots,d-1\right\}$. (These are just the eigenbases of the generalized Z- and X-Pauli operators.) Denote the projections onto these bases by $\mathcal{Z}$ and $\mathcal{X}$, respectively:

$$\mathcal{Z}(\rho) = \sum_z |z\rangle\langle z|\rho|z\rangle\langle z|,$$

$$\mathcal{X}(\rho) = \sum_x |\hat{x}\rangle\langle\hat{x}|\rho|\hat{x}\rangle\langle\hat{x}|.$$

The first uncertainty relation is by Christandl and Winter (2005): for a bipartite quantum state ρ_{AB} such that ρ_A is maximally mixed,

$$I(A:B)_{\mathcal{Z}\otimes\mathrm{id}(\rho)} + I(A:B)_{\mathcal{X}\otimes\mathrm{id}(\rho)} \leqslant I(A:B)_\rho, \tag{4}$$

where id refers to the identity map on the second system (B), while on the first (A) one of the basis projections $\mathcal{Z}$ or $\mathcal{X}$ acts.

The second is by Renes and Boileau (2009), who show similarly that for any tripartite state ρ_{ABC},

$$S(A|B)_{\mathcal{Z}\otimes\mathrm{id}(\rho)} + S(A|C)_{\mathcal{X}\otimes\mathrm{id}(\rho)} \geqslant \log d. \tag{5}$$

Note that this directly reduces to (3) for trivial systems B and C—which is why Renes and Boileau (2009) conjectured the following inequality when $\mathcal{Z}$ and $\mathcal{X}$ are more generally the projections onto two arbitrary bases $\mathcal{A}$ and $\mathcal{B}$, respectively:

$$S(A|B)_{\mathcal{Z}\otimes\mathrm{id}(\rho)} + S(A|C)_{\mathcal{X}\otimes\mathrm{id}(\rho)} \geqslant -\log c(\mathcal{A},\mathcal{B}).$$

This relation has indeed been proven recently by Berta *et al* (2009).

3. More than two measurements

We now review the known results for entropic uncertainty relations for more than two measurement settings. Little is known in this scenario, except for a number of special cases. In particular, it is an interesting open question whether strong uncertainty relations even exist for a small constant number of measurement settings and more than two measurement outcomes. As pointed out already, this is conceivable because unlike canonically conjugate variables, which come in pairs, there are generally more than two mutually unbiased observables.

3.1. Random choice of bases

First of all, it may not be at all obvious that strong uncertainty relations can even be obtained at all for more than two measurement settings, independent of the number of measurement outcomes. We will use $\mathcal{B}_j = \{U_j|x\rangle \mid x \in \{0, \ldots, d-1\}\}$ where $|x\rangle$ forms an orthonormal basis for $\mathcal{H}$ to denote the basis obtained by rotating the standard basis into the basis determined by the unitary U_j. It was shown in Hayden *et al* (2004) that $L = (\log d)^4$ unitaries U_j chosen from the Haar measure randomly and independently obey

$$\frac{1}{L}\sum_{j=1}^{L} H(\mathcal{B}_j|\rho) \geqslant \log d - O(1) = (\log d)\left(1 - O\left(\frac{1}{\log d}\right)\right)$$

with high probability, and for sufficiently large dimension d. It is important to note that the number of measurement settings is not constant but depends on the dimension.

3.2. Mutually unbiased bases

Now that we know that it is in principle possible to obtain reasonably strong uncertainty relations, can we construct explicit measurements for which we obtain such relations? Recall that it is a necessary condition for bases to be mutually unbiased in order to obtain a maximally strong uncertainty relation in the first place. Given the fact that if we have two measurement settings, choosing the measurement bases to be mutually unbiased leads to maximally strong uncertainty relations, it may be tempting to conclude that choosing our measurements to be mutually unbiased is in general also a sufficient condition. Perhaps surprisingly, this is not the case.

3.2.1. For $d+1$ mutually unbiased bases. We first consider the case of all $d+1$ mutually unbiased bases, for which we *can* obtain strong uncertainty relations. In particular, Ivanovic (1992) and Sanchez (1993) have shown that for the mutually unbiased bases $\mathcal{B}_1, \ldots, \mathcal{B}_{d+1}$ we have for any state ρ

$$\frac{1}{d+1}\sum_{j=1}^{d+1} H(\mathcal{B}_j|\rho) \geqslant \log(d+1) - 1. \tag{6}$$

If the dimension d is even, this can further be improved to (Sanchez-Ruiz 1995)

$$\frac{1}{d+1}\sum_{j=1}^{d+1} H(\mathcal{B}_j|\rho) \geqslant \frac{1}{d+1}\left[\frac{d}{2}\log\left(\frac{d}{2}\right) + \left(\frac{d}{2}+1\right)\log\left(\frac{d}{2}+1\right)\right].$$

In dimension $d = 2$, the latter bound gives $2/3$, which is tight for the mutually unbiased bases given by the eigenvectors of the Pauli matrices X, Z and Y. The case of $d = 2$ was also addressed separately in Sanchez-Ruiz (1998).

It is worth noting that the first bound (6) is in fact obtained by first lower bounding the Shannon entropy $H(\cdot)$ by the collision entropy $H_2(\cdot)$, and then one proves that

$$\frac{1}{d+1}\sum_{j=1}^{d+1} H_2(\mathcal{B}_j|\rho) \geqslant \log(d+1) - 1. \tag{7}$$

This inequality can also be proven using the fact that a full set of mutually unbiased bases forms a two-design (Ballester and Wehner 2007), and we provide a completely elementary proof of this inequality in the appendix. Interestingly, it has been shown (Wootters and Sussman 2007) that the states ρ minimizing the lhs of (7) are states, which are invariant under a unitary transformation that permutes the mutually unbiased bases as discussed in section 1.3.

3.2.2. For less than $d+1$ mutually unbiased bases. What about less than $d+1$ mutually unbiased bases? First of all, note that it is easy to see that we do not always obtain a maximally strong uncertainty relation in this setting. Consider dimension $d = 3$ and three mutually unbiased bases $\mathcal{B}_1$, $\mathcal{B}_2$ and $\mathcal{B}_3$ given by the eigenvectors of X_3, Z_3 and X_3Z_3, respectively. Then a simple calculation shows that for example for the state $|\psi\rangle = (|1\rangle - |2\rangle)/\sqrt{2}$ we have $H(\mathcal{B}_j||\psi\rangle) = 1$ for all bases $j \in \{1, 2, 3\}$ and hence

$$\frac{1}{3}\sum_{j=1}^{3} H(\mathcal{B}_j||\psi\rangle) = 1 < \frac{2}{3}\log 3.$$

In DiVincenzo *et al* (2004) (see the eprint version), numerical work on three and more mutually unbiased bases in prime dimensions up to 29 is reported, which are consistent with a behavior of $(1 - O(1/k))(\log d)$ of the average entropy lower bound. The mutually unbiased bases are taken as a subset of the MUBs constructed via the generalized Pauli matrices in prime power dimension.

Trivial bounds for more than two and less than $d+1$ can be derived quite easily. For example, for any number of mutually unbiased bases $\mathcal{B}_1, \ldots, \mathcal{B}_L$ we obtain by combining (3) for each pair of bases $\mathcal{B}_i$ and $\mathcal{B}_j$ that

$$\frac{1}{L}\sum_{j=1}^{L} H(\mathcal{B}_j|\rho) \geqslant \frac{\log d}{2}. \tag{8}$$

As shown in the appendix, it is also easy to see that

$$\frac{1}{L}\sum_{j=1}^{L} H(\mathcal{B}_j|\rho) \geqslant -\log\frac{L+d-1}{dL}.$$

Curiously, it turns out (Ballester and Wehner 2007) that in square prime power dimensions $d = p^{2\ell}$ there exist up to $L = p^{\ell} + 1$ MUBs derived from the generalized Pauli matrices for

which we obtain extremely weak uncertainty relations! In particular, we have for any such set of MUBs that the lower bound of (8) can be attained[5], that is,

$$\min_{\rho} \frac{1}{L} \sum_{j} H(\mathcal{B}_j|\rho) = \frac{\log d}{2} .$$

Furthermore, the same is true for *all* mutually unbiased bases derived from Latin squares. These results clearly show that mutual unbiasedness is *not* enough to obtain strong uncertainty relations. Combined with the numerical results from above, we also note that the dimension d, as well as the choice of mutually unbiased bases may indeed matter. In Ballester and Wehner (2007) it was noted that the set of mutually unbiased bases derived from the generalized Pauli matrices for which we obtain weak uncertainty relations are exactly those which are separable across the space $\mathbb{C}^{p^\ell} \otimes \mathbb{C}^{p^\ell}$. However, we can now conclude from the results of Wootters and Sussman (2007) that there is nothing inherently special about these separable bases, since there exists a unitary U that maps them to a set of entangled (i.e. non-product) bases (see section 1.3). It has also been shown by Ambainis (2006) that for any three bases from the 'standard' mutually unbiased bases construction in prime dimension the lower bound cannot exceed $\left(\frac{1}{2} + o(1)\right) \log d$, for large dimensions. For dimensions of the form $4k+3$ and $8k+5$ no further assumption is needed, but the proof assumes the generalized Riemann hypothesis for dimensions of the form $8k+1$. Furthermore, for any $0 \leqslant \epsilon \leqslant 1/2$, there always exist $k = d^\epsilon$ many of these bases such that the lower bound cannot be larger than $(\frac{1}{2} + \epsilon + o(1)) \log d$. Tight uncertainty relations for the min-entropy have also been shown recently for $O(\log d)$ MUBs with special symmetry properties in dimension $d = 2^n$ (Mandayam and Wehner 2009). It remains an interesting open question to show tight uncertainty relations for all mutually unbiased bases.

3.3. Anti-commuting observables

Maximally strong uncertainty relations are known to exist for any number of measurement settings L, if we limit ourselves to 2 outcomes. These uncertainty relations are derived for generators of a Clifford algebra (Dietz 2006, Lounesto 2001), which has many beautiful geometrical properties. For any integer n, the free real associative algebra generated by $\Gamma_1, \ldots, \Gamma_{2n}$, subject to the anti-commutation relations

$$\{\Gamma_j, \Gamma_k\} = \Gamma_j \Gamma_k + \Gamma_k \Gamma_j = 2\delta_{jk} \mathbb{1}, \tag{9}$$

is called a *Clifford algebra*. It has a unique representation by Hermitian matrices on n qubits (up to unitary equivalence). This representation can be obtained via the famous Jordan–Wigner transformation (Jordan and Wigner 1928):

$$\Gamma_{2j-1} = Z^{\otimes(j-1)} \otimes X \otimes \mathbb{1}^{\otimes(n-j)},$$

$$\Gamma_{2j} \quad = Z^{\otimes(j-1)} \otimes Y \otimes \mathbb{1}^{\otimes(n-j)},$$

for $j = 1, \ldots, n$, where we use X, Y and Z to denote the Pauli matrices. An additional such matrix can be found by taking the product $\Gamma_0 := \Gamma_1 \Gamma_2 \ldots \Gamma_{2n}$, which is sometimes known as the pseudo-scalar. To see how such operators are observables with two measurement outcomes,

[5] And many more if one relaxes the condition of mutual unbiasedness to approximate unbiasedness, using the techniques of Hayden *et al* (2004).

note that the eigenvalues of Γ_i always come in pairs: Let $|\eta\rangle$ be an eigenvector of Γ_i with eigenvalue λ. From $\Gamma_i^2 =$ we have that $\lambda^2 = 1$. Note that both ± 1 occur since we have $\Gamma_i(\Gamma_j|\eta\rangle) = -\lambda\Gamma_j|\eta\rangle$. We can therefore express each Γ_i as

$$\Gamma_i = \Gamma_i^0 - \Gamma_i^1,$$

where Γ_i^0 and Γ_i^1 are projectors onto the positive and negative eigenspace of Γ_i, respectively. Furthermore, note that we have for $i \neq j$

$$\mathrm{Tr}(\Gamma_i\Gamma_j) = \tfrac{1}{2}\,\mathrm{Tr}(\Gamma_i\Gamma_j + \Gamma_j\Gamma_i) = 0.$$

That is, all such operators are orthogonal. To gain some intuition of why such operators may give good uncertainty relations, we also note that the two eigenspaces are equally large, i.e., $\mathrm{rank}(\Gamma_i^0) = \mathrm{rank}(\Gamma_i^1)$ for all i, and that the positive and negative eigenspaces of such operators are mutually unbiased (analogous to bases), since for all $i \neq j$, and an arbitrary eigenvector $|\psi_i\rangle$ of Γ_i,

$$\langle\psi_i|\Gamma_j|\psi_i\rangle = \langle\psi_i|\Gamma_j^0|\psi_i\rangle - \langle\psi_i|\Gamma_j^1|\psi_i\rangle = 0.$$

Hence, if we were to measure the maximally mixed state on the positive eigenspace of Γ_j with any of the other observables, the probability of obtaining a measurement outcome of 0 is the same as for obtaining outcome 1. For simplicity, we will write $H_\alpha(\Gamma_j|\rho) := H_\alpha(\{\Gamma_j^0, \Gamma_j^1\}|\rho)$.

It was shown (Wehner and Winter 2008) that the following maximally strong uncertainty relation holds for any set of anti-commuting observables $\mathcal{S} \subseteq \{\Gamma_j \mid j \in \{0, \ldots, 2n\}\}$

$$\min_\rho \frac{1}{|\mathcal{S}|}\sum_{\Gamma_j\in\mathcal{S}} H(\Gamma_j|\rho) = 1 - \frac{1}{|\mathcal{S}|}.$$

For dimension $d = 2$, this reduces to an uncertainty relation for the mutually unbiased bases given by the eigenvectors of X, Z and Y, respectively. This result is based on a form of 'meta-uncertainty relation' which has also been shown in a different context in Toth and Guehne (2005). For the collision entropy, the bound becomes

$$\min_\rho \frac{1}{|\mathcal{S}|}\sum_{\Gamma_j\in\mathcal{S}} H_2\left(\Gamma_j|\rho\right) = 1 - \log\left(1 + \frac{1}{|\mathcal{S}|}\right) \sim 1 - \frac{\log e}{|\mathcal{S}|},$$

and for the min-entropy we have

$$\min_\rho \frac{1}{|\mathcal{S}|}\sum_{\Gamma_j\in\mathcal{S}} H_\infty\left(\Gamma_j|\rho\right) = 1 - \log\left(1 + \frac{1}{\sqrt{|\mathcal{S}|}}\right). \tag{10}$$

Interestingly, uncertainty relations for anti-commuting observables can also be used to prove Tsirelson's bound (Ver Steeg and Wehner 2009).

It is not known how to extend this result to more than two measurement outcomes. One may conjecture that the generalized Clifford algebra generated by operators $\Lambda_1, \ldots, \Lambda_n$, where for all $i \neq j$ we have

$$\Lambda_i\Lambda_j = \omega\Lambda_j\Lambda_i,$$

with $\omega = \mathrm{e}^{2\Pi\mathrm{i}/\ell}$ may give strong uncertainty relations for measurements with ℓ measurement outcomes. However, the example for X_3, Z_3 and X_3Z_3 given above, and numerical evidence for higher dimensions refute this conjecture.

4. Applications

Uncertainty relations for measurements in different bases have recently played an important role in proving security of cryptographic protocols in the bounded (Damgaard *et al* 2007) and noisy-storage model (König *et al* 2009, Wehner *et al* 2008), respectively. Here, uncertainty relations are used to bound the information that a cheating party has about bits which are encoded into several possible bases, where the choice of basis is initially unknown to him. The simplest example is an encoding of a single bit $x_j \in \{0, 1\}$ into either the computational (as $|x_i\rangle$) or Hadamard basis (as $H|x_j\rangle$). Suppose we choose the bit x_j, as well as the basis uniformly at random, and suppose further that the cheating party is allowed to perform any measurement on the encoded qubit giving him some classical information K. After his measurement, we provide him with the basis information Θ. It can be shown using a purification argument, that we can turn the uncertainty relation for the min-entropy for the computational $\mathcal{B}_1$ and Hadamard basis $\mathcal{B}_2$ (see (10))

$$\frac{1}{2}\left(H_\infty(\mathcal{B}_1|\rho) + H_\infty(\mathcal{B}_2|\rho)\right) \geqslant -\log\left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right),$$

into the following bound for the adversary's knowledge about the bit X_j given K and the basis information Θ

$$H_\infty(X_j|K\Theta) \geqslant -\log\left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right).$$

Intuitively, the idea behind such a purification argument is to imagine that we send half of an EPR pair to the cheating party instead of one of the BB84 states. By performing a measurement, the cheating party then prepares a state on our end which we then measure in the different bases, bringing us back to our original setting. The conditional min-entropy thereby has a very intuitive interpretation as $H_\infty(X_j|K\Theta) = -\log P_{\text{guess}}(X_j|K\Theta)$, where $P_{\text{guess}}(X_j|K\Theta)$ is the average probability that the cheating party can guess X_j given K and Θ, maximized over all strategies (König *et al* 2008).

In a cryptographic setting, we are especially interested in the case where we repeat the encoding above many times. Suppose we choose an n-bit string $X_1, \ldots, X_n$ uniformly at random, and encode each bit in either the computational or Hadamard basis, also chosen uniformly and independently at random. Using the semidefinite programming formalism of Ballester *et al* (2008) it is easily seen (Wehner *et al* 2008) that this gives us

$$H_\infty(X_1, \ldots, X_n|K, \Theta) \geqslant -n\log\left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right),$$

where the measurement that minimizes the min-entropy is a product measurement, resulting in the final state to be a product state. In the limit of large n, it is known that for independent states, the min-entropy behaves approximately like the Shannon entropy (Renes 2005, Tomamichel *et al* 2008). This allows one to turn the uncertainty relation of Maassen and Uffink (1988) for the Shannon entropy into a better bound on the adversaries knowledge about the long string $X_1, \ldots, X_n$ in terms of the min-entropy. More precisely, it is known (Damgaard *et al* 2007) that

$$H^\epsilon_\infty(X_1, \ldots, X_n|K, \Theta) \geqslant \left(\frac{1}{2} - 2\delta\right)n$$

for $\epsilon = \exp(-\delta^2 n/(32(2+\log(1/\delta))^2))$, where H_∞^ϵ is the ϵ-smooth min-entropy defined in Renes (2005). Intuitively, this quantity behaves like the min-entropy, except with probability ϵ. We refer to König *et al* (2009) for more information, where this uncertainty relation was recently used to prove security in the noisy-storage model.

5. Open problems

Since a full set of mutually unbiased bases form a so-called two-design, it may be interesting to consider sets of bases forming a t-design for any $t > 2$. (A t-design of states is any set such that the average of any degree-t polynomial in the matrix elements of the states equals the Haar measure average of the same polynomial, see Ambainis and Emerson (2007).) Using the result of Klappenecker and Rötteler (2005) and the technique of Ballester and Wehner (2007) it is straightforward to prove an incredibly weak uncertainty relation for the Rényi entropy of order t, where the lower bound obeys $1/(1-t)\log((t!d!)/(t+d-1)!)$. Evidently, this lower bound becomes weaker for higher values of t, which is exactly the opposite of what one would hope for. It is an interesting open question, whether one can find good uncertainty relations for higher designs.

The most interesting open problem, however, is to find any sets of measurements at all for which we do obtain maximally strong uncertainty relations for more than two measurement settings, and a constant number of measurement outcomes $|\mathcal{X}| > 2$. Note that always

$$0 \leqslant c_{\{\mathcal{M}_j\}} \leqslant \left(1 - \frac{1}{L}\right) \log |\mathcal{X}|, \tag{11}$$

for any set of measurements $\{\mathcal{M}_j\}$ with outcomes in the set $\mathcal{X}$. The problem of the entropic uncertainty relations at its most general is to find an expression, or at least a lower bound, for the quantity $c_{\{\mathcal{M}_j\}}$ in 'simple' terms of the geometry of the measurements $\mathcal{M}_j$.

For measurements in different bases, which are of special interest for example in locking applications (DiVincenzo *et al* 2004), one is interested in the quantity

$$h(d; L) := \max_{\mathcal{B}_1,\ldots,\mathcal{B}_L} \min_\rho \frac{1}{L} \sum_{j=1}^{L} H(\mathcal{B}_j|\rho),$$

where the maximization is taken over bases $\mathcal{B}_1, \ldots, \mathcal{B}_L$. Note that if in dimension d there exist L mutually unbiased bases, then by virtue of (8) and the above (11),

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

and one would like to have a characterization of the sets of bases attaining the maximum.

Seeing thus the scaling of $h(d; L)$ with $\log d$, and assuming an asymptotic viewpoint of large dimension, we finally consider the quantity[6]

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

which depends now only on the number of bases L. For example, $h(2) = 1/2$, and it is clear that

$$h(L + L') \geqslant \frac{L}{L+L'} h(L) + \frac{L'}{L+L'} h(L'),$$

[6] If the limit exists; otherwise take the lim inf or lim sup, giving rise to $\underline{h}(L)$ and $\overline{h}(L)$, respectively.

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

Finally, since the existence of uncertainty relations is an intriguing aspect separating quantum theory from the classical world, it would be interesting to know whether entropic uncertainty relations can lead to an experimental test distinguishing the two settings.

Acknowledgments

We thank Andris Ambainis, Otfried Guehne, Michael Hall, Denes Petz, R Srikanth and Ronald de Wolf for useful comments and pointers. AW is supported by the UK EPSRC, by the Royal Society, the Leverhulme Trust, and by the European Commission through IP 'QAP' and STREP 'QICS'. The Centre for Quantum Technologies is funded by the Singapore Ministry of Education and the National Research Foundation as part of the Research Centres of Excellence programme. SW is supported by NSF grants PHY-04056720 and PHY-0803371.

Appendix. A bound for mutually unbiased bases

Here, we provide an alternative proof of an entropic uncertainty relation for a full set of mutually unbiased bases in dimension $d = 2^n$. This has previously been proved in Ivanovic (1992) and Sanchez (1993). We already provided an alternative proof using the fact that the set of all mutually unbiased bases forms a two-design (Ballester and Wehner 2007). The present a very simple alternative proof for dimension $d = 2^n$, which has the advantage that it neither requires the introduction of two-designs, nor the results of Larsen (1990) that were used in the previous proof by Sanchez-Ruiz (Sanchez 1993). Instead, our proof (Wehner 2008) is elementary: after choosing a convenient parametrization of quantum states, the statement follows immediately from Fourier analysis.

For the parameterization, we first introduce a basis for the space of $2^n \times 2^n$ matrices with the help of mutually unbiased bases. Recall that in dimension 2^n, we can find exactly $2^n + 1$ MUBs. Below, we will always think of an integer $j \in [d-1]$ as a bit string $j = j_1, \ldots, j_n \in \{0,1\}^n$ in the usual sense. The inner product of $j \in [d-1]$ and a string $x = x_1, \ldots, x_n \in \{0,1\}^n$ is then the bit wise inner product of the two bit strings modulo two $j \cdot x = \sum_k j_k x_k \bmod 2$. We will also write $j \oplus j'$ to denote the bitwise x or of strings j and j'. Suppose now that we are given a set of $d+1$ MUBs

$$\mathcal{Z} = \{\mathcal{B}_1, \ldots, \mathcal{B}_{d+1}\},$$

with $\mathcal{B}_b = \{|x_b\rangle \mid x \in \{0,1\}^n\}$. We can then construct an orthogonal basis of the $d \times d$ Hermitian matrices as follows:

Lemma A.1. *Consider the Hermitian matrices*

$$S_b^j = \sum_{x \in \{0,1\}^n} (-1)^{j \cdot x} |x_b\rangle\langle x_b|,$$

for $b \in [d+1]$, $j \in [d-1]$ and for all $x, x' \in \{0,1\}^n$ and $b \neq b' \in [d+1]$ we have $|\langle x_b | x'_{b'}\rangle|^2 = 1/d$. Then the set $\{\mathbb{1} \cup \{S_b^j | b \in [d+1], j \in [d-1]\}$ forms a basis for the space of $d \times d$ matrices, where for all j and b, S_b^j is traceless and $(S_b^j)^2 = \mathbb{1}$.

Proof. First, note that we have $(d+1)(d-1)+1 = d^2$ matrices. We now show that they are all orthogonal. Note that

$$\mathrm{Tr}(S_b^j) = \sum_{x\in\{0,1\}^n} (-1)^{j\cdot x} = 0,$$

since $j \neq 0$, and hence S_b^j is traceless. Hence $\mathrm{Tr}(\mathbb{1} S_b^j) = 0$. Furthermore,

$$\mathrm{Tr}(S_b^j S_{b'}^{j'}) = \sum_{x,x'\in\{0,1\}^n} (-1)^{j\cdot x}(-1)^{j'\cdot x'} |\langle x_b|x'_{b'}\rangle|^2. \tag{A.1}$$

For $b \neq b'$, equation (A.1) gives us $\mathrm{Tr}(S_b^j S_{b'}^{j'}) = (1/d)\left(\sum_x (-1)^{j\cdot x}\right)\left(\sum_{x'}(-1)^{j'\cdot x'}\right) = 0$, since $j, j' \neq 0$. For $b = b'$, but $j \neq j'$, we get $\mathrm{Tr}(S_b^j S_{b'}^{j'}) = \sum_x (-1)^{(j\oplus j')\cdot x} = 0$ since $j \oplus j' \neq 0$.

Finally, $(S_b^j)^2 = \sum_{xx'}(-1)^{j\cdot x}(-1)^{j\cdot x'}|x_b\rangle\langle x_b||x'_b\rangle\langle x'_b| = \mathbb{1}$. □

Since $\{\mathbb{1}, S_b^j\}$ form a basis for the $d \times d$ matrices, we can thus express the state ρ of a d-dimensional system as

$$\rho = \frac{1}{d}\left(\mathbb{1} + \sum_{b\in[d+1]}\sum_{j\in[d-1]} s_b^j S_b^j\right),$$

for some coefficients $s_b^j \in \mathbb{R}$. It is now easy to see that

Lemma A.2. *Let ρ be a pure state parameterized as above. Then*

$$\sum_{b\in[d+1]}\sum_{j\in[d-1]} (s_b^j)^2 = d-1.$$

Proof. If ρ is a pure state, we have $\mathrm{Tr}(\rho^2) = 1$. Hence

$$\begin{aligned}\mathrm{Tr}(\rho^2) &= \frac{1}{d^2}\left(\mathrm{Tr}(\mathbb{1}) + \sum_{b\in[d+1]}\sum_{j\in[d-1]} (s_b^j)^2 \mathrm{Tr}(\mathbb{1})\right)\\ &= \frac{1}{d}\left(1 + \sum_b\sum_j (s_b^j)^2\right) = 1,\end{aligned}$$

from which the claim follows. □

Lemma A.3. *Let $|x_b\rangle$ be the xth basis vector of the bth MUB. Then for any state ρ*

$$\mathrm{Tr}(|x_b\rangle\langle x_b|\rho) = \frac{1}{d}\left(1 + \sum_{j\in[d-1} (-1)^{j\cdot x} s_b^j\right).$$

Proof. We have

$$\mathrm{Tr}(|x_b\rangle\langle x_b|\rho) = \frac{1}{d}\left(\mathrm{Tr}(|x_b\rangle\langle x_b|) + \sum_{b',j} s^j_{b'}\mathrm{Tr}(S^j_{b'}|x_b\rangle\langle x_b|)\right).$$

Suppose $b \neq b'$. Then $\mathrm{Tr}(S^j_{b'}|x_b\rangle\langle x_b|) = (1/d)\sum_{x'}(-1)^{j\cdot x'} = 0$, since $j \neq 0$. Suppose $b = b'$. Then $\mathrm{Tr}(S^j_{b'}|x_b\rangle\langle x_b|) = \sum_{x'}(-1)^{j\cdot x'}|\langle x_b|x'_b\rangle|^2 = (-1)^{j\cdot x}$, from which the claim follows. □

We are now ready to prove an entropic uncertainty relation for L mutually unbiased bases.

Theorem A.4. *Let $\mathcal{S} = \{\mathcal{B}_1, \ldots, \mathcal{B}_L\} \subseteq \mathcal{Z}$ be a set of mutually unbiased bases in dimension $d = 2^n$. Then*

$$\frac{1}{L}\sum_{b\in[L]} H_2(\mathcal{B}_b, |\Psi\rangle) \geqslant -\log\frac{L+d-1}{dL}.$$

Proof. First, note that we can define functions $f_b(j) = s^j_b$ for $j \in [d-1]$ and $f_b(0) = 1$. Then $\hat{f}_b(x) = (1/\sqrt{d})(\sum_{j\in\{0,\ldots,d-1\}}(-1)^{j\cdot x}s^j_b)$ is the Fourier transform of f_b and $(1/\sqrt{d})\hat{f}_b(x) = \mathrm{Tr}(|x_b\rangle\langle x_b|\rho) = |\langle x_b|\Psi\rangle|^2$ by lemma A.3. Thus

$$\begin{aligned}
\frac{1}{L}\sum_{b\in[L]} H_2(\mathcal{B}_b, |\Psi\rangle) &= -\frac{1}{L}\sum_{b\in[L]}\log\sum_{x\in\{0,1\}^n}|\langle x_b|\Psi\rangle|^4 \\
&\geqslant -\log\frac{1}{dL}\sum_b\sum_x \hat{f}_b(x)^2 \\
&= -\log\frac{1}{dL}\sum_b\left(1+\sum_j (s^j_b)^2\right) \\
&= -\log\frac{1}{dL}(L+d-1),
\end{aligned}$$

where the first inequality follows from Jensen's inequality and the concavity of log. The next equality follows from Parseval's equality, and the last follows from the fact that $|\Psi\rangle$ is a pure state and lemma A.2. □

Corollary A.5. *Let $\mathcal{S} = \{\mathcal{B}_1, \ldots, \mathcal{B}_L\}$ be a set of mutually unbiased bases. Then*

$$\frac{1}{L}\sum_{b\in[L]} H(\mathcal{B}_b||\Psi\rangle) \geqslant -\log\frac{L+d-1}{dL}.$$

In particular, for a full set of $L = d+1$ MUBs we obtain $\frac{1}{L}\sum_b H(\mathcal{B}_b||\Psi\rangle) \geqslant \log(d+1) - 1$.

Proof. This follows immediately from theorem A.4 and the fact that $H(\cdot) \geqslant H_2(\cdot)$. □

It is interesting to note that this bound is the same that arises from interpolating between the results of Sanchez-Ruiz (1993) and Maassen and Uffink (1988) as was done by Azarchs (2004). This bound has more recently been rediscovered by Wu *et al* (2009).

References

Ambainis A 2009 *Limits on entropic uncertainty relations for 3 and more MUBs* arXiv:0909.3720

Ambainis A and Emerson J 2007 *Proc. 22nd Annu. IEEE Conf. on Computational Complexity (CCC'07)* pp 129–40 arXiv:quant-ph/0701126

Azarchs A 2004 Entropic uncertainty relations for incomplete sets of mutually unbiased observables. arXiv:quant-ph/0412083

Ballester M and Wehner S 2007 *Phys. Rev.* A **75** 022319

Ballester M, Wehner S and Winter A 2008 *IEEE Trans. Inf. Theory* **54** 4183

Bandyopadhyay S, Boykin P, Roychowdhury V and Vatan F 2002 *Algorithmica* **34** 512

Beckner W 1975 *Ann. Math.* **102** 159

Berta M, Christandl M, Colbeck R, Renes J and Renner R 2009 An entropic uncertainty relation with quantum side information. arXiv:0909.0950

Białynicki-Birula I 1984 *Phys. Lett.* A **103** 253

Białynicki-Birula I 2006 *Phys. Rev.* A **74** 052102

Białynicki-Birula I and Madajczyk J L 1985 *Phys. Lett.* A **108** 384

Białynicki-Birula I and Mycielski J 1975 *Commun. Math. Phys.* **44** 129

Christandl M and Winter A 2005 Uncertainty, monogamy and locking of quantum correlations. arXiv:quant-ph/0501090

Cover T M and Thomas J A 1991 *Elements of Information Theory* (New York: Wiley)

Damgaard I, Fehr S, Renner R, Salvail L and Schaffner C 2007 A tight high-order entropic uncertainty relation with applications in the bounded quantum-storage model *Proc. CRYPTO 2007*

Damgaard I, Fehr S, Salvail L and Schaffner C 2005 *Proc. 46th IEEE FOCS* pp 449–58

Deutsch D 1983 *Phys. Rev. Lett.* **50** 631

Dietz K 2006 *J. Phys. A: Math. Gen.* **36** 1433

DiVincenzo D, Horodecki M, Leung D, Smolin J and Terhal B 2004 *Phys. Rev. Lett.* **92** 067902

Dodonov V V and Man'ko V I 1989 Invariants and the evolution of nonstationary quantum Systems *Proc. Lebedev Physics Institute* vol 183 ed M A Markov (Commack, NY: Nova Science) pp 3–101

Ghirardi G, Marinatto L and Romano R 2003 *Phys. Lett.* A **317** 32

Gibilisco P, Hiai F and Petz D 2009 *IEEE Trans. Inf. Theory* **55** 439

Grassl M 2004 *Proc. ERATO Conf. Quantum Information Science* pp 60–1 (arXiv:quant-ph/0406175)

Guehne O 2004 *Phys. Rev. Lett.* **92** 117903

Hall M J W 1997 *Phys. Rev.* A **55** 100

Hall M J W 2008 *J. Phys. A: Math. Gen.* **41** 255301

Hayden P, Leung D, Shor P and Winter A 2004 *Commun. Math. Phys.* **250** 371

Heisenberg W 1927 *Z. Phys.* **43** 172

Hirschmann I I 1957 *Am. J. Math.* **79** 152

Ivanovic I D 1992 *J. Phys. A: Math. Gen.* **25** 363

Jordan P and Wigner E 1928 *Z. Phys.* **47** 631

Klappenecker A and Rötteler M 2004 *Int. Conf. on Finite Fields and Applications (Fq7) (Lecture Notes in Computer Science* vol 2948) (New York: Springer) pp 137–44

Klappenecker A and Rötteler M 2005 *Proc. IEEE Int. Symp. on Information Theory* pp 1740–4

Koashi M 2005 Simple security proof of quantum key distribution via uncertainty principle arXiv: quant-ph/0505108

König R, Renner R and Schaffner C 2008 The operational meaning of min- and max-entropy arXiv:0807.1338

König R, Wehner S and Wullschleger J 2009 Unconditional security in the noisy-storage model arXiv:0906.1030

Kraus K 1987 *Phys. Rev.* D **35** 3070

Krishna M and Parthasarathy K R 2002 *Ind. J. Stat.* A **64** (arXiv:quant-ph/0110025)

Landau H J and Pollack H O 1961 *Bell Syst. Tech. J.* **40** 65

Larsen U 1990 *J. Phys. A: Math. Gen.* **23** 1041
Lawrence J, Brukner C and Zeilinger A 2002 *Phys. Rev.* A **65** 032320
Lounesto P 2001 *Clifford Algebras and Spinors* (Cambridge: Cambridge University Press)
Maassen H and Uffink J 1988 *Phys. Rev. Lett.* **60** 1103
Majernik V and Majernikova E 2001 *Rep. Math. Phys.* **47** 381
Mandayam P and Wehner S 2009 in preparation
Massar S 2007 *Phys. Rev.* A **76** 042114
Partovi M H 1983 *Phys. Rev. Lett.* **50** 24
Rajagopal A K 1995 *Phys. Lett.* A **205** 32
Rastegin A E 2008a Comment on 'uncertainty relations for positive-operator-valued measures' arXiv:0810.0038
Rastegin A E 2008b arXiv:0807.2691
Rastegin A E 2008c arXiv:0805.1777
Renes J M and Boileau J-C 2009 *Phys. Rev. Lett.* **103** 020402
Renner R 2005 Security of quantum key distribution *PhD Thesis* ETH Zurich (arXiv:quant-ph/0512258)
Rényi A 1960 *Proc. 4th Berkeley Symp. on Mathematics, Statistics and Probability* pp 547–61
Riesz M 1929 *Acta Math.* **49** 465
Robertson H 1929 *Phys. Rev.* **34** 163
Sanchez J 1993 *Phys. Lett.* A **173** 233
Sanchez-Ruiz J 1995 *Phys. Lett.* A **201** 125
Sanchez-Ruiz J 1998 *Phys. Lett.* A **244** 189
Shannon C E 1948 *Bell Syst. Tech. J.* **27** 379
Srikanth R and Banerjee S 2009 *Eur. Phys. J.* D **53** 217
Tomamichel M, Colbeck R and Renner R 2008 A fully quantum asymptotic equipartition property. arXiv:0811.1221
Toth G and Guehne O 2005 *Phys. Rev.* A **72** 022340
Tsallis C 1988 *J. Stat. Phys.* **51** 479
Ver Steeg G and Wehner S 2009 *Quantum Inf. Comput.* **9** 801
de Vicente J I and Sanchez-Ruiz J 2008 *Phys. Rev.* A **77** 042110
Wehner S 2008 Cryptography in a quantum world *PhD Thesis* University of Amsterdam (arXiv:0806.3483)
Wehner S, Schaffner C and Terhal B M 2008 *Phys. Rev. Lett.* **100** 220502
Wehner S and Winter A 2008 *J. Math. Phys.* **49** 062105
Wocjan P and Beth T 2005 *Quantum Inf. and Comput.* **5** 93
Wootters W and Fields B 1989 *Ann. Phys.* **191** 368
Wootters W K and Sussman D M 2007 arXiv:0704.1277
Wu S, Yu S and Molmer K 2009 *Phys. Rev.* A **79** 022104
Zauner G 1999 Quantendesigns—Grundzüge einer nichtkommutativen designtheorie *PhD Thesis* Universität Wien