Entropic uncertainty relations and their applications

Coles, Patrick J.; Berta, Mario; Tomamichel, Marco; Wehner, Stephanie

DOI
10.1103/RevModPhys.89.015002

Publication date
2017

Document Version
Final published version

Published in
Reviews of Modern Physics

Entropic uncertainty relations and their applications

Patrick J. Coles[*]

Institute for Quantum Computing and Department of Physics and Astronomy, University of Waterloo, N2L3G1 Waterloo, Ontario, Canada

Mario Berta[†]

Institute for Quantum Information and Matter, California Institute of Technology, Pasadena, California 91125, USA

Marco Tomamichel[‡]

School of Physics, The University of Sydney, Sydney, NSW 2006, Australia

Stephanie Wehner[§]

QuTech, Delft University of Technology, 2628 CJ Delft, Netherlands

(published 6 February 2017)

Heisenberg's uncertainty principle forms a fundamental element of quantum mechanics. Uncertainty relations in terms of entropies were initially proposed to deal with conceptual shortcomings in the original formulation of the uncertainty principle and, hence, play an important role in quantum foundations. More recently, entropic uncertainty relations have emerged as the central ingredient in the security analysis of almost all quantum cryptographic protocols, such as quantum key distribution and two-party quantum cryptography. This review surveys entropic uncertainty relations that capture Heisenberg's idea that the results of incompatible measurements are impossible to predict, covering both finite- and infinite-dimensional measurements. These ideas are then extended to incorporate quantum correlations between the observed object and its environment, allowing for a variety of recent, more general formulations of the uncertainty principle. Finally, various applications are discussed, ranging from entanglement witnessing to wave-particle duality to quantum cryptography.

DOI: 10.1103/RevModPhys.89.015002

CONTENTS

[*]pcoles@uwaterloo.ca
[†]berta@caltech.edu
[‡]marco.tomamichel@sydney.edu.au
[§]s.d.c.wehner@tudelft.nl

I. INTRODUCTION

Quantum mechanics has revolutionized our understanding of the world. Relative to classical mechanics, the most dramatic change in our understanding is that the quantum world (our world) is inherently unpredictable.

By far the most famous statement of unpredictability is Heisenberg's uncertainty principle (Heisenberg, 1927), which we treat here as a statement about preparation uncertainty. Roughly speaking, it states that it is impossible to prepare a quantum particle for which both position and momentum are sharply defined. Operationally, consider a source that consistently prepares copies of a quantum particle in the same way, as shown in Fig. 1. For each copy, suppose we randomly measure either its position or its momentum (but we never attempt to measure both quantities for the same particle[1]). We record the outcomes and sort them into two sequences associated with the two different measurements. The uncertainty principle states that it is impossible to predict both the outcome of the position and the momentum measurements: at least one of the two sequences of outcomes will be unpredictable. More precisely, the better such a preparation

[1]Section I.A notes other uncertainty principles that involve consecutive or joint measurements.

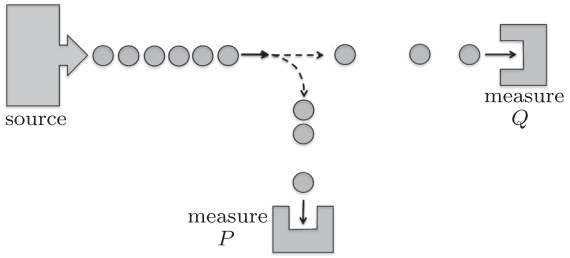


FIG. 1. Physical scenario relevant to preparation uncertainty relations. Each incoming particle is measured using either measurement P or measurement Q, where the choice of the measurement is random. An uncertainty relation says we cannot predict the outcomes of both P and Q. If we can predict the outcome of P well, then we are necessarily uncertain about the outcome of measurement Q, and vice versa.

procedure allows one to predict the outcome of the position measurement, the more uncertain the outcome of the momentum measurement will be, and vice versa.

An elegant aspect of quantum mechanics is that it allows for simple quantitative statements of this idea, i.e., constraints on the predictability of observable pairs like position and momentum. These quantitative statements are known as uncertainty relations. It is worth noting that Heisenberg's original argument, while conceptually enlightening, was heuristic. The first, rigorously proven uncertainty relation for position Q and momentum P is due to Kennard (1927). It establishes that [see also the work of Weyl (1928)]

$$\sigma(Q)\sigma(P) \geq \frac{\hbar}{2}, \tag{1}$$

where $\sigma(Q)$ and $\sigma(P)$ denote the standard deviations of the position and momentum, respectively, and $\hbar$ is the reduced Planck constant.

We now know that Heisenberg's principle applies much more generally, not only to position and momentum. Other examples of pairs of observables obeying an uncertainty relation include the phase and excitation number of a harmonic oscillator, the angle and the orbital angular momentum of a particle, and orthogonal components of spin angular momentum. In fact, for arbitrary observables[2] X and Z, Robertson (1929) showed that

$$\sigma(X)\sigma(Z) \geq \tfrac{1}{2}|\langle\psi|[X,Z]|\psi\rangle|, \tag{2}$$

where $[\cdot,\cdot]$ denotes the commutator. Note a distinct difference between Eqs. (1) and (2): the right-hand side of the former is a constant whereas that of the latter can be state dependent, an issue that we discuss more in Sec. II.

These relations have a beauty to them and also give conceptual insight. Equation (1) identifies $\hbar$ as a fundamental limit to our knowledge. More generally Eq. (2) identifies the commutator as the relevant quantity for determining how large the knowledge trade-off is for two observables. One could argue that a reasonable goal in our studies of uncertainty in quantum mechanics should be to find simple, conceptually insightful statements like these.

If this problem was only of fundamental importance, it would be a well-motivated one. Yet in recent years there is new motivation to study the uncertainty principle. The rise of quantum information theory has led to new applications of quantum uncertainty, for example, in quantum cryptography. In particular quantum key distribution is already commercially marketed and its security crucially relies on Heisenberg's uncertainty principle. (We discuss various applications in Sec. VI.) There is a clear need for uncertainty relations that are directly applicable to these technologies.

In Eqs. (1) and (2), uncertainty has been quantified using the standard deviation of the measurement results. This is, however, not the only way to express the uncertainty principle. It is instructive to consider what preparation uncertainty means in the most general setting. Suppose we prepared a state ρ on which we can perform two (or more) possible measurements labeled by θ. Let us use x to label the outcomes of such measurement. We can then identify a list of (conditional) probabilities

$$S_\rho = \{p(x|\theta)_\rho\}_{x,\theta}, \tag{3}$$

where $p(x|\theta)_\rho$ denotes the probability of obtaining measurement outcome x when performing the measurement θ on the state ρ. Quantum mechanics predicts restrictions on the set S_ρ of allowed conditional probability distributions that are valid for all or a large class of states ρ. Needless to say, there are many ways to formulate such restrictions on the set of allowed distributions.

In particular, information theory offers a very versatile, abstract framework that allows us to formalize notions like uncertainty and unpredictability. This theory is the basis of modern communication technologies and cryptography and has been successfully generalized to include quantum effects. The preferred mathematical quantity to express uncertainty in information theory is entropy. Entropies are functionals on random variables and quantum states that aim to quantify their inherent uncertainty. Among a myriad of such measures, we mainly restrict our attention to the Boltzmann-Gibbs-Shannon entropy (Boltzmann, 1872; Gibbs, 1876; Shannon, 1948) and its quantum generalization, the von Neumann entropy (von Neumann, 1932). Because of their importance in quantum cryptography, we also consider Rényi entropic measures (Rényi, 1961) such as the min-entropy. Entropy is a natural measure of uncertainty, perhaps even more natural than the standard deviation, as we argue in Sec. II.

Can the uncertainty principle be formulated in terms of entropy? This question was first brought up by Everett (1957) and answered in the affirmative by Hirschman (1957) who considered the position and momentum observables, formulating the first *entropic uncertainty relation*. This was later improved by Beckner (1975) and Białynicki-Birula and Mycielski (1975), who obtained[3]

[2]More precisely, Robertson's relation refers to observables with bounded spectrum.

[3]More precisely, the right-hand side of Eq. (4) should be $\log(e\pi\hbar/l_Q l_P)$, where l_Q and l_P are length and momentum scales, respectively, chosen to make the argument of the logarithm dimensionless. Throughout this review, all logarithms are base 2.

$$h(Q) + h(P) \geq \log(e\pi\hbar), \tag{4}$$

where h is the differential entropy [defined in Eq. (7)]. Białynicki-Birula and Mycielski (1975) also showed that Eq. (4) is stronger than, and hence implies, Kennard's relation (1).

The extension of the entropic uncertainty relation to observables with finite spectrum[4] was given by Deutsch (1983), and later improved by Maassen and Uffink (1988) following a conjecture by Kraus (1987). The result of Maassen and Uffink (1988) is arguably the most well-known entropic uncertainty relation. It states that

$$H(X) + H(Z) \geq \log\frac{1}{c}, \tag{5}$$

where H is Shannon's entropy (see Sec. III.A for definition), and c denotes the maximum overlap between any two eigenvectors of the X and Z observables. Just as Eq. (2) established the commutator as an important parameter in determining the uncertainty trade-off for standard deviation, Eq. (5) established the maximum overlap c as a central parameter in entropic uncertainty.

While these articles represent the early history of entropic uncertainty relations, there has recently been an explosion of work on this topic. One of the most important recent advances concerns a generalization of the uncertainty paradigm that allows the measured system to be correlated to its environment in a nonclassical way. Entanglement between the measured system and the environment can be exploited to reduce the uncertainty of an observer (with access to the environment) below the usual bounds.

To explain this extension, let us introduce a modern formulation of the uncertainty principle as a so-called guessing game, which makes such extensions of the uncertainty principle natural and highlights their relevance for quantum cryptography. As outlined in Fig. 2, we imagine that an observer Bob can prepare an arbitrary state ρ_A which he will send to a referee Alice. Alice then randomly chooses to perform one of two (or more) possible measurements, where we use Θ to denote her choice of measurement. She records the outcome K. Finally, she tells Bob the choice of her measurement, i.e., she sends him Θ. Bob's task is to guess Alice's measurement outcome K (given Θ).

The uncertainty principle tells us that if Alice makes two incompatible measurements, then Bob cannot guess Alice's outcome with certainty for both measurements. This corresponds precisely to the notion of preparation uncertainty. It is indeed intuitive why such uncertainty relations form an important ingredient in proving the security of quantum cryptographic protocols, as we explore in detail in Sec. VI. In the cryptographic setting ρ_A will be sent by an adversary trying to break a quantum cryptographic protocol. If Alice's measurements are incompatible, there is no way for the adversary to know the outcomes of both possible measurements with certainty—no matter what state he prepares.

[4]The relation applies to nondegenerate observables on a finite-dimensional Hilbert space (see Sec. III.B).

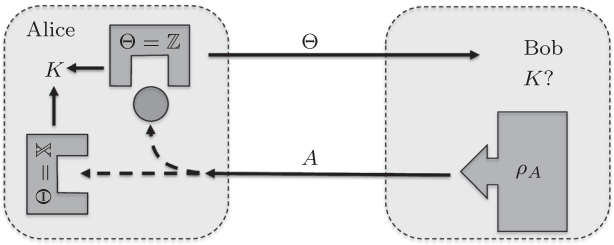


FIG. 2. Diagram showing a guessing game with players Alice and Bob. First, Bob prepares A in state ρ_A and sends it to Alice. Second, Alice measures either $\mathbb{X}$ or $\mathbb{Z}$ with equal probability and stores the measurement choice in the bit Θ. Third, Alice stores the measurement outcome in bit K and reveals the measurement choice Θ to Bob. Bob's task is to guess K (given Θ). Entropic uncertainty relations like the Maassen-Uffink relation (5) can be understood as fundamental constraints on the optimal guessing probability.

The formulation of uncertainty relations as guessing games also makes it clear that there is an important twist to such games: What if Bob prepares a bipartite state ρ_{AB} and sends only the A part to Alice? That is, what if Bob's system is correlated with Alice's? Or, adopting the modern perspective of information, what if Bob has a nontrivial amount of *side information* about Alice's system? Traditional uncertainty relations implicitly assume that Bob has only classical side information. For example, he may possess a classical description of the state ρ_A or other details about the preparation. However, modern uncertainty relations—for example those derived by Berta *et al.* (2010) improving on work by Christandl and Winter (2005) and Renes and Boileau (2009)—allow Bob to have *quantum* rather than classical information about the state. As was already observed by Einstein, Podolsky, and Rosen (1935), Bob's uncertainty can vanish in this case (in the sense that he can correctly guess Alice's measurement outcome K in the game described above).

We devote Sec. IV to such modern uncertainty relations. It is these relations that will be of central importance in quantum cryptography, where the adversary may have gathered quantum and not just classical information during the course of the protocol that may reduce his uncertainty.

A. Scope of this review

Two survey articles partially discuss the topic of entropic uncertainty relations. Białynicki-Birula and Rudnicki (2011) take a physics perspective and cover continuous variable entropic uncertainty relations and some discretized measurements. In contrast, Wehner and Winter (2010) take an information-theoretic perspective and discuss entropic uncertainty relations for discrete (finite) variables with an emphasis on relations that involve more than two measurements.

These reviews predate many recent advances in the field. For example, neither review covers entropic uncertainty relations that take into account quantum correlations with the environment of the measured system. Moreover,

applications of entropic uncertainty relations are only marginally discussed in both of these reviews. Here we discuss both physical and information-based applications. We therefore aim to give a comprehensive treatment of all of these topics in one reference, with the hope of benefiting some of the quickly emerging technologies that exploit quantum information.

There is an additional aspect of the uncertainty principle known as *measurement uncertainty*; see, e.g., Ozawa (2003), Hall (2004), Busch, Heinonen, and Lahti (2007), and Busch, Lahti, and Werner (2014a). This includes (1) joint measurability, the concept that there exist pairs of observables that cannot be measured simultaneously, and (2) measurement disturbance, the concept that there exist pairs of observables for which measuring one causes a disturbance of the other. Measurement uncertainty is a debated topic of current research. We focus our review article on the concept of preparation uncertainty, although we briefly mention entropic approaches to measurement uncertainty in Sec. VII.C.

II. RELATION TO STANDARD DEVIATION APPROACH

Traditional formulations of the uncertainty principle, for example, the ones due to Kennard and Robertson, measure uncertainty in terms of the standard deviation. In this section we argue why we think entropic formulations are preferable. For further discussion we refer to Uffink (1990).

A. Position and momentum uncertainty relations

For the case of position and momentum observables, the strength of the entropic formulation can be seen from the fact that the entropic uncertainty relation in Eq. (4) is stronger and in fact implies the standard deviation relation (1). Following Białynicki-Birula and Mycielski (1975), we formally show that

$$h(Q)+h(P)\geq \log(e\pi) \Rightarrow \sigma(Q)\sigma(P)\geq \tfrac{1}{2} \tag{6}$$

for all states, where here and henceforth in this article we work in units such that $\hbar = 1$. Let us consider a random variable Q governed by a probability density $\Gamma(q)$, and the differential entropy

$$h(Q) = -\int_{-\infty}^{\infty} \Gamma(q)\log\Gamma(q)dq. \tag{7}$$

In the following we assume that this quantity is finite. Gaussian probability distributions,

$$\Gamma(q) = \frac{1}{\sqrt{2\pi\sigma(Q)^2}}\exp\left(\frac{-(q-\bar{q})^2}{2\sigma(Q)^2}\right), \tag{8}$$

where $\bar{q}$ denotes the mean, are special in the following sense: for a fixed standard deviation $\sigma(Q)$, distributions of the form of Eq. (8) maximize the entropy in Eq. (7). It is a simple exercise to show this using variational calculus with Lagrange multipliers.

It is furthermore straightforward to insert Eq. (8) into (7) to calculate the entropy of a Gaussian distribution

$$h(Q) = \log\sqrt{2\pi e\sigma(Q)^2} \quad \text{(Gaussian)}. \tag{9}$$

Since Gaussians maximize the entropy, the following inequality holds:

$$h(Q) \leq \log\sqrt{2\pi e\sigma(Q)^2} \quad \text{(in general)}. \tag{10}$$

Now consider an arbitrary quantum state for a particle's translational degree of freedom, which gives rise to random variables P and Q for the position and momentum, respectively. Let us insert the resulting relations into Eq. (4) to find

$$\log[2\pi e\sigma(Q)\sigma(P)] = \log\sqrt{2\pi e\sigma(Q)^2} + \log\sqrt{2\pi e\sigma(P)^2} \tag{11}$$

$$\geq h(Q)+h(P) \tag{12}$$

$$\geq \log(e\pi). \tag{13}$$

By comparing the left- and right-hand sides of Eq. (11) and noting that the logarithm is a monotonic function, we see that Eq. (11) implies (1), and hence so does (4).

It is worth noting that Eq. (10) is a strict inequality if the distribution is non-Gaussian, and hence Eq. (4) is strictly stronger than (1) if the quantum state is non-Gaussian. While quantum mechanics textbooks often present Eq. (1) as the fundamental statement of the uncertainty principle, it is clear that Eq. (4) is stronger and yet not much more complicated. Furthermore, as discussed in Sec. IV the entropic formulation is more robust, allowing the relation to be easily generalized to situations involving correlations with the environment.

B. Finite spectrum uncertainty relations

As noted in Sec. I, both the standard deviation and the entropy have been applied to formulate uncertainty relations for observables with a finite spectrum. However, it is largely unclear how the most popular formulations, Robertson's (2) and Maassen-Uffink's (5), are related. It remains an interesting open question whether there exists a formulation that unifies these two formulations. However, there is an important difference between Eqs. (2) and (5) in that the former has a bound that depends on the state, while the latter depends only on the two observables.

Example 1. Consider Eq. (2) for the case of a spin-1/2 particle, where $X = |0\rangle\langle 1| + |1\rangle\langle 0|$ and $Z = |0\rangle\langle 0| - |1\rangle\langle 1|$, corresponding to the x and z axes of the Bloch sphere. Then the commutator is proportional to the Y Pauli operator and the right-hand side of Eq. (2) reduces to $(1/2)|\langle Y\rangle|$. Hence, Eq. (2) gives a trivial bound for all states that lie in the x-z plane of the Bloch sphere. For the eigenstates of X and Z, this bound is tight since one of the two uncertainty terms is zero, and hence the trivial bound is a (perhaps undesirable) consequence of the fact that the left-hand side involves a *product* (rather than a sum) of uncertainties. However, for any other states in the x-z plane, neither uncertainty is zero. This implies that Eq. (2) is *not tight* for these states.

This example illustrates a weakness of Robertson's relation for finite-dimensional systems—it gives trivial bounds for certain states, even when the left-hand side is nonzero. Schrödinger (1930) slightly strengthened Robertson's bound by adding an additional state-dependent term that helps to get rid of the artificial trivial bound discussed in example 1. Likewise, Maccone and Pati (2014) recently proved a state-dependent bound on the sum (not the product) of the two variances, and this bound also removes the trivial behavior of Robertson's bound. Furthermore, one still may be able to obtain a nonvanishing state-independent bound using standard deviation uncertainty measures in the finite-dimensional case. For example, Busch, Lahti, and Werner (2014b) considered the qubit case and obtained a state-independent bound on the sum of the variances.

The state-dependent nature of Robertson's bound was noted by Deutsch (1983) and used as motivation for entropic uncertainty relations, which do not suffer from this weakness. However, this discussion suggests that this issue might be avoided while still using standard deviation as the uncertainty measure. On the other hand, there are more important issues that we now discuss.

C. Advantages of entropic formulation

From a practical perspective, a crucial advantage of entropic uncertainty relations are their applications throughout quantum cryptography. However, let us now mention several other reasons why we think that the entropic formulation of the uncertainty principle is advantageous over the standard deviation formulation.

1. Counterintuitive behavior of standard deviation

While the standard deviation is, of course, a good measure of deviation from the mean, its interpretation as a measure of uncertainty has been questioned. It has been pointed out, for example, by Białynicki-Birula and Rudnicki (2011), that the standard deviation behaves somewhat strangely for some simple examples.

Example 2. Consider a spin-1 particle with equal probability $\Pr(s_z) = 1/3$ to have each of the three possible values of Z angular momentum $s_z \in \{-1, 0, 1\}$. The standard deviation of the Z angular momentum is $\sigma(Z) = \sqrt{2/3}$. Now suppose we gain information about the spin such that we now know that it definitely does not have the value $s_z = 0$. The new probability distribution is $\Pr(1) = \Pr(-1) = 1/2$, $\Pr(0) = 0$. We might expect the uncertainty to decrease, since we have gained information about the spin, but in fact the standard deviation increases, the new value being $\sigma(Z) = 1$.

We remark that the different behavior of standard deviation and entropy for spin angular momentum was recently highlighted by Dammeier, Schwonnek, and Werner (2015), in the context of states that saturate the relevant uncertainty relation.

Białynicki-Birula and Rudnicki (2011) noted an example for a particle's spatial position that is analogous to example 2.

Example 3. Consider a long box of length L, centered at $Q = 0$, with two small boxes of length a attached to the two ends of the long box, as depicted in Fig. 3. Suppose we know that a classical particle is confined to the two small end boxes,

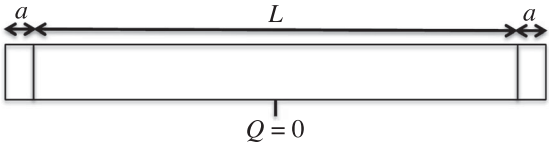


FIG. 3. Illustration for example 3, where a particle is initially confined to the two small boxes at the end and excluded from the long middle box. Then the particle is allowed to go free into the middle box.

i.e., with equal probability it is one of the two small boxes. The standard deviation of the position is $\sigma(Q) \approx L/2$, assuming that $L \gg a$. Now suppose the barriers that separate the end boxes from the middle box are removed, and the particle is allowed to move freely between all three boxes. Intuitively one might expect that the uncertainty of the particle's position is now larger, since we now know nothing about where the particle is inside the three boxes. However, the new standard deviation is actually smaller: $\sigma(Q) \approx L/\sqrt{12}$.

Entropies, on the other hand, do not have this counterintuitive behavior, due to properties discussed later. Finally, let us note a somewhat obvious issue that, in some cases, a quantitative label (and hence the standard deviation) does not make sense, as illustrated in the following example.

Example 4. Consider a neutrino's flavor, which is often modeled as a three-outcome observable with outcomes "electron," "muon," or "tau." As this is a nonquantitative observable, the standard deviation does not make sense in this context. Nevertheless, it is of interest to quantify the uncertainty about the neutrino flavor, i.e., how difficult it is to guess the flavor, which is naturally captured by the notion of entropy.

2. Intuitive entropic properties

Deutsch (1983) emphasized that the standard deviation can change under a simple relabeling of the outcomes. For example, if one were to assign quantitative labels to the outcomes in example 4 and then relabel them, the standard deviation would change. In contrast, the entropy is invariant under relabeling of outcomes, because it naturally captures the amount of information about a measurement outcome.

Furthermore, there is a nice monotonic property of entropy in the following sense. Suppose one does a random relabeling of the outcomes. One can think of this as a relabeling plus added noise, which naturally tends to spread the probability distribution out over the outcomes. Intuitively, a relabeling with the injection of randomness should never decrease the uncertainty. This property, nondecreasing under random relabeling, was highlighted by Friedland, Gheorghiu, and Gour (2013) as a desirable property of an uncertainty measure. Indeed, entropy satisfies this property. On the other hand, the physical process in example 3 can be modeled mathematically as a random relabeling. Hence, we see the contrast in behavior between entropy and standard deviation.

Monotonicity under random relabeling is actually a special case of an even more powerful property. Think of the random relabeling as due to the fact that the observer is denied access to an auxiliary register that stores the information about which relabeling occurred. If the observer had access to the register,

then their uncertainty would remain the same, but without access their uncertainty could potentially increase, but never decrease. More generally, this idea (that losing access to an auxiliary system cannot reduce one's uncertainty) is a desirable and powerful property of uncertainty measures known as the *data-processing inequality*. It is arguably a defining property of entropy measures, or more precisely, conditional entropy measures as discussed in Sec. IV.B. Furthermore this property is central in proving entropic uncertainty relations (Coles *et al.*, 2012).

3. Framework for correlated quantum systems

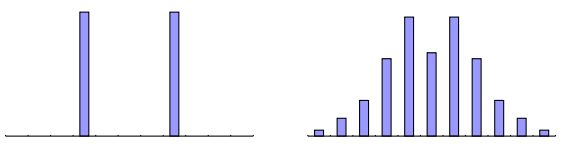
Entropy provides a robust mathematical framework that can be generalized to deal with correlated quantum systems. For example, the entropy framework allows us to discuss the uncertainty of an observable from the perspective of an observer who has access to part of the environment of the system or to quantify quantum correlations like entanglement between two quantum systems. This requires measures of conditional uncertainty, namely, conditional entropies. We highlight the utility of this framework in Sec. IV. A similar framework for standard deviation has not been developed.

4. Operational meaning and information applications

Perhaps the most compelling reason to consider entropy as the uncertainty measure of choice is that it has operational significance for various information-processing tasks. The standard deviation, in contrast, does not play a significant role in information theory. This is because entropy abstracts from the physical representation of information, as one can see from the following example.

Example 5. Consider the two probability distributions in Fig. 4. They have the same standard deviation but different entropy. The distribution in Fig. 4(a) has 1 bit of entropy since only two events are possible and occur with equal probability. If we want to record data from this random experiment this will require exactly 1 bit of storage per run. On the other hand, the distribution in Fig. 4(b) has approximately 3 bits of entropy and the recorded data cannot be compressed to less than 3 bits per run. Clearly, entropy has operational meaning in this context while standard deviation fails to distinguish these random experiments.

Entropies have operational meaning for tasks such as randomness extraction (extracting perfect randomness from a partially random source) and data compression (sending minimal information to someone to help them guess the output of a partially random source). It is precisely these operational meanings that make entropic uncertainty relations useful for proving the security of quantum key distribution and other cryptographic tasks. We discuss such applications in Sec. VI.



(a) low entropy distribution (b) high entropy distribution

FIG. 4. Two probability distributions with the same standard deviation but different entropy, as explained in example 5.

The operational significance of entropy allows one to frame entropic uncertainty relations in terms of guessing games (see Secs. III.F and IV.D.1). These are simple yet insightful tasks where one party is trying to guess the outcome of another party's measurements (see the description in Fig. 2). Such games make it clear that the uncertainty principle is not just abstract mathematics; rather it is relevant to physical tasks that can be performed in a laboratory.

III. UNCERTAINTY WITHOUT A MEMORY SYSTEM

Historically, entropic uncertainty relations were first studied for position and momentum observables. However, to keep the discussion mathematically simple we begin here by introducing entropic uncertainty relations for finite-dimensional quantum systems, and we defer the discussion of infinite dimensions to Sec. V. It is worth noting that many physical systems of interest are finite dimensional, such as photon polarization, neutrino flavor, and spin angular momentum.

In this section, we consider uncertainty relations for a single system A. That is, there is no memory system. We emphasize that all uncertainty relations with a memory system can also be applied to the situation without.

A. Entropy measures

Let us consider a discrete random variable X distributed according to the probability distribution P_X. We assume that X takes values in a finite set $\mathcal{X}$. For example, this set could be binary values $\{0,1\}$ or spin states $\{\uparrow,\downarrow\}$. In general, we associate the random variable X with the outcome of a particular measurement. This random variable can take values $X=x$, where x is a specific instance of a measurement outcome that can be obtained with probability $P_X(X=x)$. However, entropies depend only on the probability law P_X and not on the specific labels of the elements in the set $\mathcal{X}$. Thus, we will in the following just assume this set to be of the form $[d] \coloneqq \{1,2,3,\ldots,d\}$, where $d=|X|$ stands for the cardinality of the set $\mathcal{X}$.

1. Surprisal and Shannon entropy

Following Shannon (1948), we first define the *surprisal* of the event $X=x$ distributed according to P_X as $-\log P_X(x)$, often also referred to as *information content*. As its name suggests, the information content of $X=x$ gets larger when the event $X=x$ is less likely, i.e., when $P_X(x)$ is smaller. In particular, deterministic events have no information content at all, which is indeed intuitive since we learn nothing by observing an event that we are assured will happen with certainty. In contrast, the information content of very unlikely events can get arbitrarily large. Based on this intuition, the Shannon entropy is defined as

$$H(X) \coloneqq \sum_x P_X(x) \log \frac{1}{P_X(x)} \tag{14}$$

and quantifies the average information content of X. It is therefore a measure of the uncertainty of the outcome of the random experiment described by X. The Shannon entropy is by far the best-known measure of uncertainty, and it is the one most commonly used to express uncertainty relations.

2. Rényi entropies

However, for some applications it is important to consider other measures of uncertainty that give more weight to events with high or low information content, respectively. For this purpose we employ a generalization of the Shannon entropy to a family of entropies introduced by Rényi (1961). The family includes several important special cases which we discuss individually. These entropies have found many applications in cryptography and information theory (see Sec. VI) and have convenient mathematical properties.[5]

The Rényi entropy of order α is defined as

$$H_\alpha(X) := \frac{1}{1-\alpha}\log\sum_x P_X(x)^\alpha, \tag{15}$$

for $\alpha \in (0,1)\cup(1,\infty)$, and as the corresponding limit for $\alpha \in \{0,1,\infty\}$. For $\alpha = 1$ the limit yields the Shannon entropy,[6] and the Rényi entropies are thus a proper generalization of the Shannon entropy.

The Rényi entropies are monotonically decreasing as a function of α. Entropies with $\alpha > 1$ give more weight to events with high surprisal. The collision entropy $H_{\mathrm{coll}} := H_2$ is given by

$$\begin{aligned} H_{\mathrm{coll}}(X) &= -\log p_{\mathrm{coll}}(X), \\ \text{where } p_{\mathrm{coll}}(X) &:= \sum_x P_X(x)^2 \end{aligned} \tag{16}$$

is the collision probability, i.e., the probability that two independent instances of X are equal. The *min-entropy* $H_{\min} := H_\infty$ is of special significance in many applications. It characterizes the optimal probability of correctly guessing the value of X in the following sense:

$$\begin{aligned} H_{\min}(X) &= -\log p_{\mathrm{guess}}(X), \\ \text{where } p_{\mathrm{guess}}(X) &:= \max_x P_X(x). \end{aligned} \tag{17}$$

Clearly, the optimal guessing strategy is to bet on the most likely value of X, and the winning probability is then given by the maximum in Eq. (17). The min-entropy can also be seen as the minimum surprisal of X.

The Rényi entropies with $\alpha < 1$ give more weight to events with small surprisal. Noteworthy examples are the *max-entropy* $H_{\max} := H_{1/2}$ and

$$H_0(X) = \log|\{x : P_X(x) > 0\}|, \tag{18}$$

where the latter is simply the logarithm of the support of P_X.

3. Examples and properties

For all the Rényi entropies, $H_\alpha(X) = 0$ if and only if the distribution is perfectly peaked, i.e., $P_X(x) = 1$ for some particular value x. On the other hand, the distribution $P_X(x) = |X|^{-1}$ is uniform if and only if the entropy takes its maximal value $H_\alpha(X) = \log|X|$.

The Rényi entropies can take on very different values depending on the parameter α as the following example, visualized in Fig. 5, shows.

Example 6. Consider a distribution of the form

$$P_X(x) = \begin{cases} \frac{1}{2} & \text{for } x = 1, \\ \frac{1}{2(|X|-1)} & \text{else,} \end{cases} \tag{19}$$

so that we have

$$\begin{aligned} H_{\min}(X) &= \log 2, \\ \text{whereas} \qquad H(X) &= \log 2 + \tfrac{1}{2}\log(|X|-1) \end{aligned} \tag{20}$$

is arbitrarily large as $|X| \geq 2$ increases. This is of particular relevance in cryptographic applications where $H_{\min}(X)$, and not $H(X)$, characterizes how difficult it is to guess a secret X. As we will see later, $H_{\min}(X)$ precisely determines the number of random bits that can be obtained from X.

Consider two probability distributions P_X and Q_Y and define $d = \max\{|X|,|Y|\}$. Now let us reorder the probabilities in P_X into a vector $P_X^\downarrow$ such that $P_X^\downarrow(1) \geq P_X^\downarrow(2) \geq \cdots \geq P_X^\downarrow(d)$, padding with zeros if necessary. Analogously arrange the probabilities in Q_Y into a vector $Q_Y^\downarrow$. We say P_X majorizes Q_Y and write $P_X \succ Q_Y$ if

$$\sum_{x=1}^{y} P_X^\downarrow(x) \geq \sum_{x=1}^{y} Q_Y^\downarrow(x), \quad \text{for all } y \in [d]. \tag{21}$$

Intuitively, the fact that P_X majorizes Q_Y means that P_X is less spread out than Q_Y. For example, the distribution

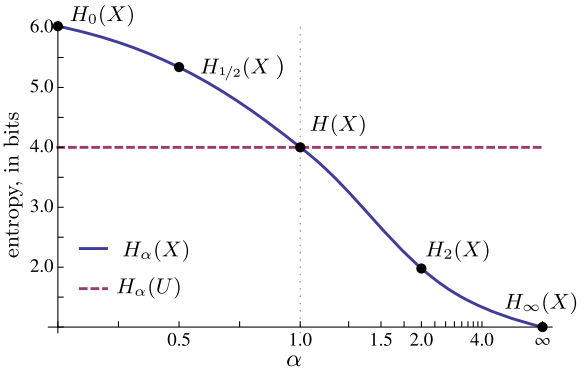


FIG. 5. Rényi entropies of X with probability distribution as in example 6 with $|X| = 65$ compared to a uniform random variable U on 4 bits.

[5]Another family of entropies that are often encountered are the Tsallis entropies (Tsallis, 1988). They have not found an operational interpretation in cryptography or information theory. Thus, we defer the discussion of Tsallis entropies until Sec. VII.A.

[6]It is a simple exercise to apply L'Hôpital's rule to Eq. (15) in the limit $\alpha \to 1$.

$\{1,0,\ldots,0\}$ majorizes every other distribution, while the uniform distribution $\{|X|^{-1},\ldots,|X|^{-1}\}$ is majorized by every other distribution.

One of the most fundamental properties of the Rényi entropies is that they are Schur concave (Marshall, Olkin, and Arnold, 2011), meaning that they satisfy

$$H_\alpha(X) \le H_\alpha(Y) \quad \text{if } P_X \succ Q_Y. \tag{22}$$

This has an important consequence. Let $Y = f(X)$ for some (deterministic) function f. In other words, Y is obtained by processing X using the function f. The random variable Y is then governed by the push forward Q_Y of P_X, that is

$$Q_Y(y) = \sum_{x:f(x)=y} P_X(x). \tag{23}$$

Clearly $P_X \prec Q_Y$ and thus we have $H_\alpha(X) \ge H_\alpha(Y)$. This corroborates our intuition that the input of a function is at least as uncertain as its output. If Z is just a reordering of X, or more generally if f is injective, then the two entropies are equal.

Finally we note that if two random variables X and Y are independent, we have

$$H_\alpha(XY) = H_\alpha(X) + H_\alpha(Y). \tag{24}$$

This property is called *additivity*.

B. Preliminaries

1. Physical setup

The physical setup used throughout the remainder of this section is as follows. We consider a quantum system A that is measured in either one of two (or more) bases. The initial state of the system A is represented by a density operator ρ_A or more formally a positive semidefinite operator with unit trace acting on a finite-dimensional Hilbert space A. The measurements for now are given by two orthonormal bases of A. An orthonormal basis is a set of unit vectors in A that are mutually orthogonal and span the space A. The two bases are denoted by sets of rank-1 projectors,

$$\mathbb{X} = \{|\mathbb{X}^x\rangle\langle\mathbb{X}^x|\}_x \quad \text{and} \quad \mathbb{Z} = \{|\mathbb{Z}^z\rangle\langle\mathbb{Z}^z|\}_z. \tag{25}$$

We use projectors to keep the notation consistent as we later consider more general measurements. This induces two random variables X and Z corresponding to the measurement outcomes that result from measuring in the bases $\mathbb{X}$ and $\mathbb{Z}$, respectively. These are governed by the following probability laws, given by the Born rule. We have

$$P_X(x) = \langle\mathbb{X}^x|\rho_A|\mathbb{X}^x\rangle \quad \text{and} \quad P_Z(z) = \langle\mathbb{Z}^z|\rho_A|\mathbb{Z}^z\rangle, \tag{26}$$

respectively. We also note that $|X| = |Z| = d$, which is the dimension of the Hilbert space A.

2. Mutually unbiased bases

Before delving into uncertainty relations, let us consider pairs of observables such that perfect knowledge about observable $\mathbb{X}$ implies complete ignorance about observable $\mathbb{Z}$. We say that such observables are unbiased or mutually unbiased. For any finite-dimensional space there exist pairs of orthonormal bases that satisfy this property. More precisely, two orthonormal bases $\mathbb{X}$ and $\mathbb{Z}$ are mutually unbiased bases (MUBs) if

$$|\langle\mathbb{X}^x|\mathbb{Z}^z\rangle|^2 = \frac{1}{d}, \quad \forall\ x,z. \tag{27}$$

In addition, a set of n orthonormal bases $\{\mathbb{X}_j\}$ is said to be a set of n MUBs if each basis $\mathbb{X}_j$ is mutually unbiased to every other basis $\mathbb{X}_k$, with $k \ne j$, in the set.

Example 7. For a qubit the eigenvectors of the Pauli operators,

$$\sigma_{\mathbb{X}} := |0\rangle\langle 1| + |1\rangle\langle 0|, \tag{28}$$

$$\sigma_{\mathbb{Y}} := -i|0\rangle\langle 1| + i|1\rangle\langle 0|, \tag{29}$$

$$\sigma_{\mathbb{Z}} := |0\rangle\langle 0| - |1\rangle\langle 1|, \tag{30}$$

form a set of three MUBs.

In Appendix A we discuss constructions for sets of MUBs in higher dimensional spaces. We also point to Durt *et al.* (2010) for a review on this topic.

C. Measuring in two orthonormal bases

1. Shannon entropy

Based on the pioneering work by Deutsch (1983) and following a conjecture of Kraus (1987), Maassen and Uffink (1988) formulated entropic uncertainty relations for measurements of two complementary observables. Their best-known relation uses the Shannon entropy to quantify uncertainty. It states that, for any state ρ_A,

$$H(X) + H(Z) \ge \log\frac{1}{c} =: q_{\mathrm{MU}}, \tag{31}$$

where the measure of incompatibility is a function of the *maximum overlap* of the two measurements, namely,

$$c = \max_{x,z} c_{xz}, \quad \text{where } c_{xz} = |\langle\mathbb{X}^x|\mathbb{Z}^z\rangle|^2. \tag{32}$$

Note that q_{MU} is state independent, i.e., independent of the initial state ρ_A. This is in contrast to Robertson's bound in Eq. (2).

The bound q_{MU} is nontrivial as long as $\mathbb{X}$ and $\mathbb{Z}$ do not have any vectors in common. In this case, Eq. (31) shows that for any input density matrix there is some uncertainty in at least one of the two random variables X and Z quantified by the Shannon entropies $H(X)$ and $H(Z)$, respectively. In general we have

$$\frac{1}{d} \le c \le 1 \quad \text{and hence} \quad 0 \le q_{\mathrm{MU}} \le \log d. \tag{33}$$

For the extreme case that $\mathbb{X}$ and $\mathbb{Z}$ are MUBs, as defined in Eq. (27), the overlap matrix $[c_{xz}]$ is flat: $c_{xz} = 1/d$ for all

x and z, and the lower bound on the uncertainty then becomes maximal

$$H(X) + H(Z) \geq \log d. \tag{34}$$

Note that this is a necessary and sufficient condition, $c = 1/d$ if and only if the two bases are MUBs. Hence, MUBs uniquely give the strongest uncertainty bound here.

For general observables $\mathbb{X}$ and $\mathbb{Z}$ the overlap matrix is not necessarily flat and the asymmetry of the matrix elements c_{xz} is quantified in Eq. (32) by taking the maximum over all x, z. In order to see why the maximum entry provides some (fairly coarse) measure of the flatness of the whole matrix, note that if the maximum entry of the overlap matrix is $1/d$, then all entries in the matrix must be $1/d$. Alternative measures of incompatibility are discussed in Secs. III.C.5 and III.C.6.

2. Rényi entropies

Maassen and Uffink (1988) also showed that Eq. (31) holds more generally in terms of Rényi entropies. For any α, $\beta \geq 1/2$ with $1/\alpha + 1/\beta = 2$, we have

$$H_\alpha(X) + H_\beta(Z) \geq q_{\mathrm{MU}}. \tag{35}$$

It is easily checked that Eq. (31) in terms of the Shannon entropy is recovered for $\alpha = \beta = 1$. For $\alpha \to \infty$ with $\beta \to 1/2$ we get another interesting special case of Eq. (35) in terms of the min- and max-entropy

$$H_{\min}(X) + H_{\max}(Z) \geq q_{\mathrm{MU}}. \tag{36}$$

Since the min-entropy characterizes the probability of correctly guessing the outcome X, it is this type of relation that becomes most useful for applications in quantum cryptography and quantum information theory (see Sec. VI).

3. Maassen-Uffink proof

The original proof of Eq. (35) by Maassen and Uffink makes use of the Riesz-Thorin interpolation theorem [see, e.g., Bergh and Löfström (1976)]. Recently an alternative proof was formulated by Coles *et al.* (2011, 2012) using the monotonicity of the relative entropy under quantum channels. The latter approach is illustrated in Appendix B, where we prove the special case of the Shannon entropy relation (31). The proof is simple and straightforward. Hence, we highly recommend the interested reader to study Appendix B. The Rényi entropy relation (35) follows from a more general line of argument given in Appendix C.3.

4. Tightness and extensions

Given the simple and appealing form of the Maassen-Uffink relations (35) a natural question to ask is how tight these relations are. It is easily seen that if $\mathbb{X}$ and $\mathbb{Z}$ are MUBs, then they are tight for any of the states $\rho_A = |\mathbb{X}^x\rangle\langle\mathbb{X}^x|$ or $\rho_A = |\mathbb{Z}^z\rangle\langle\mathbb{Z}^z|$. Thus, there cannot exist a better state-independent bound if $\mathbb{X}$ and $\mathbb{Z}$ are MUBs. However, for general orthonormal bases $\mathbb{X}$ and $\mathbb{Z}$ Eqs. (35) are not necessarily tight. This issue is addressed in the following sections, where we also note that Eq. (31) can be tightened for mixed states ρ_A with a state-dependent bound.

Going beyond orthonormal bases, these relations can be extended to more general measurements, as discussed in Sec. III.D. Finally, another interesting extension considers more than two observables (which in some cases leads to tighter bounds for two observables), as discussed in Sec. III.G.

5. Tighter bounds for qubits

Various attempts have been made to strengthen the Maassen-Uffink bound, particularly in the Shannon entropy form (31). Let us begin by first discussing improvements upon (31) in the qubit case and then move on to arbitrary dimensions.

For qubits the situation is fairly simple since the overlap matrix $[c_{xz}]$ depends only on a single parameter, which we take as the maximum overlap $c = \max_{x,z} c_{xz}$. Hence, the goal is to find the largest function of c that still lower bounds the entropic sum. Significant progress along these lines was made by Sánchez-Ruiz (1998), who noted that the Maassen-Uffink bound q_{MU} could be replaced by the stronger bound

$$q_{\mathrm{SR}} := h_{\mathrm{bin}}\left(\frac{1+\sqrt{2c-1}}{2}\right). \tag{37}$$

Here $h_{\mathrm{bin}}(p) := -p\log p - (1-p)\log(1-p)$ denotes the binary entropy.

Later work by Ghirardi, Marinatto, and Romano (2003) attempted to find the optimal bound. They simplified the problem to a single-parameter optimization as

$$q_{\mathrm{opt}} := \min_\theta \left[h_{\mathrm{bin}}\left(\frac{1+\cos\theta}{2}\right) + h_{\mathrm{bin}}\left(\frac{1+\cos(\alpha-\theta)}{2}\right)\right], \tag{38}$$

where $\alpha := 2\arccos\sqrt{c}$. While it is straightforward to perform this optimization, Ghirardi, Marinatto, and Romano (2003) noted that an analytical solution could be found only for $c \gtrsim 0.7$. They showed that this analytical bound is given by

$$q_{\mathrm{G}} := 2h_{\mathrm{bin}}(b), \qquad c \gtrsim 0.7, \tag{39}$$

where

$$b := \left(\frac{1+\sqrt{c}}{2}\right). \tag{40}$$

Figure 6 shows a plot of q_{opt}, q_{SR}, and q_{MU}. In addition, this plot also shows the bound q_{maj} obtained from a majorization technique discussed in Sec. III.I.

For pairs of Rényi entropies H_α and H_β in Eq. (35), Zozor, Bosyk, and Portesi (2013) and Abdelkhalek *et al.* (2015) completely characterized the amount of uncertainty in the qubit case.

6. Tighter bounds in arbitrary dimension

Extending the qubit result from Eq. (38), de Vicente and Sánchez-Ruiz (2008) found an analytical bound in the large overlap (i.e., large c) regime

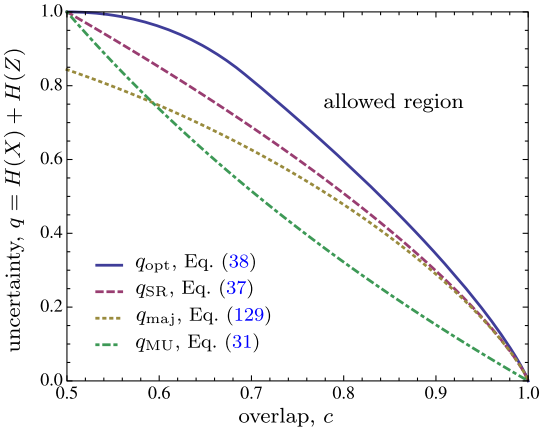


FIG. 6. Various literature bounds on entropic uncertainty for qubit orthonormal bases as a function of the maximum overlap c. The region above $q_{\rm opt}$ contains pairs (c, q) that can be achieved by quantum mechanics.

$$q_{\rm dVSR} \coloneqq 2h_{\rm bin}(b) \quad \text{for } c \gtrsim 0.7, \tag{41}$$

which is stronger than the MU bound over this range, and they also obtained a numerical improvement over MU for the range $1/2 \le c \lesssim 0.7$.

However, the situation for $d > 2$ is more complicated than the qubit case. For $d > 2$ the overlap matrix $[c_{xz}]$ depends on more parameters than simply the maximum overlap c. Recent work has focused on exploiting these other overlaps to improve upon the MU bound. For example, Coles and Piani (2014b) derived a simple improvement on $q_{\rm MU}$ that captures the role of the second-largest entry of $[c_{xz}]$, denoted c_2, with the bound

$$q_{\rm CP} \coloneqq \log\frac{1}{c} + \frac{1}{2}(1-\sqrt{c})\log\frac{c}{c_2}. \tag{42}$$

Consider the following qutrit example where $q_{\rm CP} > q_{\rm MU}$.

Example 8. Let $d = 3$ and consider the two orthonormal bases $\mathbb{X}$ and $\mathbb{Z}$ related by the unitary transformation

$$U = \begin{pmatrix} 1/\sqrt{3} & 1/\sqrt{3} & 1/\sqrt{3} \\ 1/\sqrt{2} & 0 & -1/\sqrt{2} \\ 1/\sqrt{6} & -\sqrt{2/3} & 1/\sqrt{6} \end{pmatrix}. \tag{43}$$

We have $q_{\rm MU} = \log(3/2) \approx 0.58$ while $q_{\rm CP} \approx 0.64$.

Recently, a bound similar in spirit to $q_{\rm CP}$ was obtained by Rudnicki, Puchała, and Życzkowski (2014) of the form

$$q_{\rm RPZ} \coloneqq \log\frac{1}{c} - \log\left(b^2 + \frac{c_2}{c}(1-b^2)\right). \tag{44}$$

Note that $q_{\rm RPZ} \ge q_{\rm MU}$. However, there is no clear relation between $q_{\rm CP}$ and $q_{\rm RPZ}$.

For arbitrary pairs of entropies H_α and H_β, Abdelkhalek *et al.* (2015) gave conditions on the minimizing state of Eq. (35). In particular, the minimizing state is pure and real. For measurements in the standard and Fourier basis, further conditions are obtained.

7. Tighter bounds for mixed states

Notice that Eq. (31) can be quite loose for mixed states. For example, if $\rho_A = \mathbb{1}/d$, then the left-hand side of Eq. (31) is $2\log d$, whereas the right-hand side is at most $\log d$. This looseness can be addressed by introducing a state-dependent bound that gets larger as ρ_A becomes more mixed. The mixedness of ρ_A can be quantified by the von Neumann entropy $H(\rho_A)$, which we also denote by $H(A)_\rho$, defined by

$$H(\rho_A) \coloneqq -\mathrm{tr}[\rho_A \log \rho_A] = \sum_j \lambda_j \log\frac{1}{\lambda_j}, \tag{45}$$

where an eigenvalue decomposition of the state is given by $\rho_A = \sum_j \lambda_j |\phi_j\rangle\langle\phi_j|_A$. Note that $0 \le H(\rho_A) \le \log d$, where $H(\rho_A) = 0$ for pure states and $H(\rho_A) = \log d$ for maximally mixed states. In the literature, the von Neumann entropy is sometimes also denoted using $S(A) = H(A)$. However, here we follow the more common convention in quantum information theory. We note that the entropy never decreases when applying a projective measurement $\mathbb{X} = \{|\mathbb{X}^x\rangle\langle\mathbb{X}^x|\}_x$ to ρ_A, that is,

$$H(\rho_A) \le H(X)_P \quad \text{with} \quad P_X(x) = \langle\mathbb{X}^x|\rho_A|\mathbb{X}^x\rangle. \tag{46}$$

Equation (31) was strengthened for mixed states by Berta *et al.* (2010) with the bound

$$H(X) + H(Z) \ge q_{\rm MU} + H(\rho_A). \tag{47}$$

A proof of Eq. (47) is given in Appendix B; see also Frank and Lieb (2012) for a direct matrix analysis proof. When $\mathbb{X}$ and $\mathbb{Z}$ are MUBs, this bound is tight for any state ρ_A that is diagonal in either the $\mathbb{X}$ or $\mathbb{Z}$ basis.

D. Arbitrary measurements

Many interesting measurements are not of the orthonormal basis form. For example, coarse-grained (degenerate) projective measurements are relevant to probing macroscopic systems. Also, there are other measurements that are informationally complete in the sense that their statistics allow one to reconstruct the density operator.

The most general description of measurements in quantum mechanics is that of positive operator-valued measures (POVMs). A POVM on a system A is a set of positive semidefinite operators $\{\mathbb{X}^x\}$ that sum to the identity $\sum_x \mathbb{X}^x = \mathbb{1}_A$. The number of POVM elements in the set can be much larger or much smaller than the Hilbert space dimension of the system. Physically, a POVM can be implemented as a projective measurement on an enlarged Hilbert space, e.g., as a joint measurement on the system of interest with an ancilla system.

For two POVMs $\mathbb{X} = \{\mathbb{X}^x\}_x$ and $\mathbb{Z} = \{\mathbb{Z}^z\}_z$, the general Born rule now induces the distributions

$$P_X(x) = \mathrm{tr}[\rho_A \mathbb{X}^x] \quad \text{and} \quad P_Z(z) = \mathrm{tr}[\rho_A \mathbb{Z}^z]. \tag{48}$$

Krishna and Parthasarathy (2002) proposed an incompatibility measure for POVMs using the operator norm. Namely, they considered

$$c = \max_{x,z} c_{xz} \quad \text{with} \quad c_{xz} = \|\sqrt{\mathbb{X}^x}\sqrt{\mathbb{Z}^z}\|^2, \tag{49}$$

where $\|\cdot\|$ denotes the operator norm (i.e., the maximal singular value). Using this measure they generalized Eq. (31) to the case of POVMs. That is, we still have

$$H(X) + H(Z) \geq \log\frac{1}{c}, \tag{50}$$

but now using the generalized version of c in Eq. (49). More recently, Tomamichel (2012) noted that an alternative generalization to POVMs is obtained by replacing c with

$$c' := \min\left\{\max_x \left\|\sum_z \mathbb{Z}^z\mathbb{X}^x\mathbb{Z}^z\right\|, \max_z \left\|\sum_x \mathbb{X}^x\mathbb{Z}^z\mathbb{X}^x\right\|\right\}, \tag{51}$$

and it was conjectured that c' always provides a stronger bound than c.

Indeed this conjecture was proved by Coles and Piani (2014b):

$$\left\|\sum_z \mathbb{Z}^z\mathbb{X}^x\mathbb{Z}^z\right\| \leq \max_z c_{xz}. \tag{52}$$

Hence, $c' \leq c$, implying that $\log(1/c')$ provides a stronger bound on entropic uncertainty than $\log(1/c)$.

Example 9. Consider two POVMs given by

$$\mathbb{X} = \mathbb{Z} = \tfrac{1}{2}\{|0\rangle\langle 0|, |1\rangle\langle 1|, |+\rangle\langle +|, |-\rangle\langle -|\}. \tag{53}$$

For these POVMs we find $c = 1/4$, but $c' = 3/16$ is strictly smaller.

Interestingly, a general POVM can have a nontrivial uncertainty relation on its own. That is, for some POVM $\mathbb{X}$, there may not exist any state ρ_A that has $H(X) = 0$. Krishna and Parthasarathy (2002) noted this and derived the single POVM uncertainty relation

$$H(X) \geq -\log\max_x \|\mathbb{X}^x\|. \tag{54}$$

In fact the proof is straightforward: simply apply Eq. (50) to the case where $\mathbb{Z} = \{\mathbb{1}\}$ is the trivial POVM. Equation (54) can be further strengthened by applying this approach to c' in Eq. (51), instead of c.

E. State-dependent measures of incompatibility

In most uncertainty relations we have encountered so far, the measure of incompatibility, for example, the overlap c, is a function of the measurements employed but is independent of the quantum state prior to measurement. The sole exception is the strengthened Maassen-Uffink relation in Eq. (47), where the lower bound is the sum of an ordinary, state-independent measure of incompatibility and the entropy of ρ_A. In the following, we review some uncertainty relations that use measures of incompatibility that are state dependent.

Tomamichel and Hänggi (2013) showed that the Maassen-Uffink relation (31) also holds when the overlap c is replaced by an effective overlap, denoted c^*. Informally, c^* is given by the average overlap of the two measurements on different subspaces of the Hilbert space, averaged over the probability of finding the state in the subspace. See Tomamichel and Hänggi (2013) for a formal definition of c^*. Here we discuss a simple example showing that state-dependent uncertainty relations can be significantly tighter.

Example 10. Let us apply one out of two projective measurements, either in the orthonormal basis[7]

$$\{|0\rangle, |1\rangle, |\perp\rangle\} \quad \text{or} \quad \{|+\rangle, |-\rangle, |\perp\rangle\}, \tag{55}$$

on a state ρ which has the property that $\perp$ is measured with probability at most ε. The Maassen-Uffink relation (31) gives a trivial bound as the overlap of the two bases is $c = 1$ due to the vector $|\perp\rangle$ that appears in both bases. Still, our intuitive understanding is that the uncertainty about the measurement outcome is high as long as ε is small. The *effective overlap* (Tomamichel and Hänggi, 2013) captures this intuition:

$$c^* = (1-\varepsilon)\tfrac{1}{2} + \varepsilon. \tag{56}$$

This formula can be interpreted as follows: with probability $1-\varepsilon$ we are in the subspace spanned by $|0\rangle$ and $|1\rangle$, where the overlap is $1/2$, and with probability ε we measure $\perp$ and have full overlap.

An alternative approach to state-dependent uncertainty relations was introduced by Coles and Piani (2014b). They showed that the factor $q_{\mathrm{MU}} = \log(1/c)$ in the Maassen-Uffink relation (31) can be replaced by the state-dependent factor

$$q(\rho_A) := \max\{q_X(\rho_A), q_Z(\rho_A)\}, \tag{57}$$

where

$$q_X(\rho_A) := \sum_x P_X(x)\log\frac{1}{\max_z c_{xz}}, \tag{58}$$

and $q_Z(\rho_A)$ is defined analogously to $q_X(\rho_A)$, but with x and z interchanged. Here $P_X(x)$ and c_{xz} are given by Eqs. (26) and (32), respectively. Note that this strengthens the Maassen-Uffink bound $q(\rho_A) \geq q_{\mathrm{MU}}$ since averaging $\log(1/\max_z c_{xz})$ over all x is larger than minimizing it over all x. In many cases $q(\rho_A)$ is significantly stronger than q_{MU}.

Recently, Kaniewski, Tomamichel, and Wehner (2014) derived entropic uncertainty relations in terms of the effective anticommutator of arbitrary binary POVMs $\mathbb{X} = \{\mathbb{X}^0, \mathbb{X}^1\}$ and $\mathbb{Z} = \{\mathbb{Z}^0, \mathbb{Z}^1\}$. Namely, the quantity

$$\varepsilon^* = \tfrac{1}{2}\mathrm{tr}[\rho[O_{\mathbb{X}}, O_{\mathbb{Z}}]_+] = \tfrac{1}{2}\mathrm{tr}[\rho(O_{\mathbb{X}}O_{\mathbb{Z}} + O_{\mathbb{Z}}O_{\mathbb{X}})],$$
$$\text{with} \quad O_{\mathbb{X}} = \mathbb{X}^0 - \mathbb{X}^1 \quad \text{and} \quad O_{\mathbb{Z}} = \mathbb{Z}^0 - \mathbb{Z}^1 \tag{59}$$

binary observables corresponding to the POVMs $\mathbb{X}$ and $\mathbb{Z}$, respectively. In Eq. (59), we use the notation $[\cdot,\cdot]_+$ to denote the anticommutator. We note that $\varepsilon^* \in [-1, 1]$. This results, for

[7]The diagonal states are $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$.

example, in the following uncertainty relation for the Shannon entropy:

$$H(X) + H(Z) \geq h_{\text{bin}}\left(\frac{1+\sqrt{|\varepsilon^*|}}{2}\right). \tag{60}$$

See Kaniewski, Tomamichel, and Wehner (2014) for similar uncertainty relations in terms of Rényi entropies as well as extensions to more than two measurements. Finally, for measurements acting on qubits, we find that $|\varepsilon^*| = 2c - 1$, and Eq. (60) hence reduces to the Sanchez-Ruiz bound (37).

F. Relation to guessing games

Let us now explain in detail how some of the previous relations can be interpreted in terms of a guessing game. We elaborate on the brief discussion of guessing games in Sec. I; see Fig. 2 for an illustration of the game.

The game is as follows. Suppose that Bob prepares system A in state ρ_A. He then sends A to Alice, who randomly performs either the $\mathbb{X}$ or $\mathbb{Z}$ measurement. The measurement outcome is a bit denoted as K, and Bob's task is to guess K, given that he received the basis choice denoted by $\Theta \in \{\theta_{\mathbb{X}}, \theta_{\mathbb{Z}}\}$ from Alice.

We can rewrite the Maassen-Uffink relation (31) in the following way such that the connection to the above guessing game becomes transparent. Denote the standard basis on A as $\{|k\rangle\}_{k=1}^{d}$, and let $U_{\mathbb{X}}$ and $U_{\mathbb{Z}}$, respectively, be unitaries that map this basis to the $\mathbb{X}$ and $\mathbb{Z}$ bases, i.e.,

$$|\mathbb{X}^k\rangle = U_{\mathbb{X}}|k\rangle \quad \text{and} \quad |\mathbb{Z}^k\rangle = U_{\mathbb{Z}}|k\rangle. \tag{61}$$

Then, we have

$$\tfrac{1}{2}[H(K|\Theta = \theta_{\mathbb{X}}) + H(K|\Theta = \theta_{\mathbb{Z}})] \geq \tfrac{1}{2}q_{\text{MU}}, \tag{62}$$

with the conditional probability distribution

$$P_{K|\Theta=\theta_{\mathbb{X}}}(k) \coloneqq \langle k|U_{\mathbb{X}}^{\dagger}\rho U_{\mathbb{X}}|k\rangle \quad \text{for } k \in \{1, \ldots, d\} \tag{63}$$

and similarly for $\theta_{\mathbb{Z}}$. Alternatively we can also write this as

$$H(K|\Theta) \geq \tfrac{1}{2}q_{\text{MU}} \quad \text{with} \quad \Theta \in \{\theta_{\mathbb{X}}, \theta_{\mathbb{Z}}\}, \tag{64}$$

in terms of the conditional Shannon entropy

$$H(K|\Theta) \coloneqq H(K\Theta) - H(\Theta) \tag{65}$$

$$= \tfrac{1}{2}[H(K|\Theta = \theta_{\mathbb{X}}) + H(K|\Theta = \theta_{\mathbb{X}})] \tag{66}$$

of the bipartite distribution

$$P_{K\Theta}(k, \theta_j) \coloneqq \tfrac{1}{2}\langle k|U_j^{\dagger}\rho U_j|k\rangle \quad \text{with} \quad k \in \{1, \ldots, d\}, \quad j \in \{\mathbb{X}, \mathbb{Z}\}. \tag{67}$$

That is, each measurement labeled θ_j is chosen with equal probability $1/2$ and we condition the entropy on this choice. Notice that the form in Eq. (64) is connected to the guessing game in Fig. 2. Regardless of the state ρ_A that Bob prepares, the uncertainty relation (64) implies that he will not be able to perfectly guess K if $q_{\text{MU}} > 0$. In this sense, the Maassen-Uffink relation is a fundamental constraint on one's ability to win a guessing game.

Actually, in the context of guessing games, the min-entropy is more operationally relevant than the Shannon entropy. For example, a diligent reading of Deutsch (1983) reveals

$$p_{\text{guess}}(X) \cdot p_{\text{guess}}(Z) \leq b^2, \tag{68}$$

for orthonormal bases $\mathbb{X}$ and $\mathbb{Z}$, where b is defined in Eq. (40). This relation gives an upper bound on the product of the guessing probabilities (or, equivalently, a lower bound on the sum of the min-entropies) associated with X and Z. However, to make a more explicit connection to the guessing game previously described, one wants an upper bound on the sum (or average) of the guessing probabilities, namely, the quantity

$$p_{\text{guess}}(K|\Theta) = \tfrac{1}{2}[p_{\text{guess}}(K|\Theta = \theta_{\mathbb{X}}) + p_{\text{guess}}(K|\Theta = \theta_{\mathbb{Z}})]. \tag{69}$$

Indeed, the quantity (69) has an upper bound given by (Schaffner, 2007)

$$p_{\text{guess}}(K|\Theta) \leq b \tag{70}$$

or equivalently

$$H_{\min}(K|\Theta) \geq \log\frac{1}{b}. \tag{71}$$

Example 11. For the Pauli qubit measurements $\{\sigma_{\mathbb{X}}, \sigma_{\mathbb{Z}}\}$ the min-entropy uncertainty relation (71) becomes

$$H_{\min}(K|\Theta) \geq \log\frac{2\sqrt{2}}{1+\sqrt{2}}. \tag{72}$$

We emphasize that $p_{\text{guess}}(K|\Theta)$ is precisely the probability for winning the game described in Fig. 2. Hence, the entropic uncertainty relation (71) gives the fundamental limit on winning the game. Finally, we remark that Eq. (71) is stronger than Deutsch's relation (68), due to the following argument. For the min-entropy, conditioning on the measurement choice is defined as

$$H_{\min}(K|\Theta) \coloneqq -\log\left(\frac{1}{2}\sum_{j=1,2} 2^{-H_{\min}(K|\Theta=\theta_j)}\right) \neq H_{\min}(K\Theta) - H_{\min}(\Theta) \quad \text{(in general)}, \tag{73}$$

in contrast to the Shannon entropy in Eq. (65). However, in analogy to Eq. (66), we have

$$H_{\min}(K|\Theta) \leq \frac{1}{2}\sum_{j=1,2} H_{\min}(K|\Theta = \theta_j) \tag{74}$$

due to the concavity of the logarithm. For a general discussion of conditional entropies see Sec. IV.B.

G. Multiple measurements

So far we have considered only entropic uncertainty relations quantifying the complementarity of two measurements. However, there is no fundamental reason for restricting to this setup, and in the following we discuss the more general case of L measurements. We mostly focus on special sets of measurements that generate strong uncertainty relations. This is of particular interest for various applications in quantum cryptography (see Sec. VI.C).

The notation introduced for guessing games in Sec. III.F is particularly useful in the multiple measurements setting. In this notation, for larger sets of measurements we are interested in finding lower bounds of the form

$$H(K|\Theta) \geq f(\Theta,\rho_A) > 0 \quad \text{with} \quad \Theta \in \{\theta_1,\ldots,\theta_L\}, \tag{75}$$

where, similarly to Eq. (67),

$$P_{K\Theta}(k,\theta_j) \coloneqq \frac{1}{L}\langle k|U_j^\dagger \rho U_j|k\rangle \quad \text{with} \quad k \in \{1,\ldots,d\}, \quad j \in \{1,\ldots,L\}. \tag{76}$$

Again the left-hand side of Eq. (75) might alternatively be written as

$$H(K|\Theta) = \frac{1}{L}\sum_{j=1}^{L} H(K|\Theta=\theta_j), \tag{77}$$

where the conditional probability distribution $P_{K|\Theta=\theta_j}$ is defined analogously to (63).

1. Bounds implied by two measurements

It is important to realize that the Maassen-Uffink relation (31) already implies bounds for larger sets of measurements. This is easily seen by just applying Eq. (31) to all possible pairs of measurements and adding the corresponding lower bounds.

Example 12. For the qubit Pauli measurements we find by an iterative application of the tightened Maassen-Uffink bound (47) for the measurement pairs $\{\sigma_\mathbb{X},\sigma_\mathbb{Y}\}$, $\{\sigma_\mathbb{X},\sigma_\mathbb{Z}\}$, and $\{\sigma_\mathbb{Y},\sigma_\mathbb{Z}\}$ that

$$H(K|\Theta) \geq \tfrac{1}{2} + \tfrac{1}{2}H(\rho_A) \quad \text{with} \quad \Theta \in \{\sigma_\mathbb{X},\sigma_\mathbb{Y},\sigma_\mathbb{Z}\}. \tag{78}$$

The goal of this section is to find uncertainty relations that are stronger than any bounds that can be derived directly from relations for two measurements.

2. Complete sets of MUBs

Promising candidates for deriving strong uncertainty relations are complete sets of MUBs, i.e., sets of $d+1$ MUBs (which we know to exist only in certain dimensions, see Appendix A for elaboration). Consider the qubit case in the following example.

Example 13. For the qubit Pauli measurements, we have from Sánchez-Ruiz (1995, 1998) that

$$H(K|\Theta) \geq \tfrac{2}{3} \quad \text{with} \quad \Theta \in \{\sigma_\mathbb{X},\sigma_\mathbb{Y},\sigma_\mathbb{Z}\}. \tag{79}$$

Moreover, from Coles *et al.* (2011) we can add an entropy dependent term on the right-hand side,

$$H(K|\Theta) \geq \tfrac{2}{3} + \tfrac{1}{3}H(\rho_A) \quad \text{with} \quad \Theta \in \{\sigma_\mathbb{X},\sigma_\mathbb{Y},\sigma_\mathbb{Z}\}. \tag{80}$$

Note that Eq. (80) is never a worse bound than Eq. (78) which just followed from the tightened Maassen-Uffink relation for two measurements (47). Moreover, Eq. (79) becomes an equality for any eigenstate of the Pauli measurements, while Eq. (80) becomes an equality for any state ρ_A that is diagonal in the eigenbasis of one of the Pauli measurements.

More generally, for a full set of $d+1$ MUBs in dimension d, Larsen (1990), Ivanovic (1992), and Sánchez-Ruiz (1993) showed that

$$H(K|\Theta) \geq \log(d+1) - 1 \quad \text{with} \quad \Theta \in \{\theta_1,\ldots,\theta_{d+1}\}. \tag{81}$$

This is a strong bound since the entropic term on the left-hand side can become at most $\log d$ for any number and choice of measurements. Equation (81) can be derived from an uncertainty equality for the collision entropy H_{coll}. Namely, for any quantum state ρ_A on a d-dimensional system and a full set of $d+1$ MUBs, we have (Ivanovic, 1992; Brukner and Zeilinger, 1999; Ballester and Wehner, 2007)

$$H_{\text{coll}}(K|\Theta) = \log(d+1) - \log\left(2^{-H_{\text{coll}}(\rho_A)} + 1\right) \quad \text{with} \quad \Theta \in \{\theta_1,\ldots,\theta_{d+1}\}, \tag{82}$$

where for the collision entropy the conditioning on the measurement choice is defined as

$$H_{\text{coll}}(K|\Theta) \coloneqq -\log\left(\frac{1}{L}\sum_{j=1}^{L} 2^{-H_{\text{coll}}(K|\Theta=\theta_j)}\right) \neq H_{\text{coll}}(K\Theta) - H_{\text{coll}}(\Theta) \quad \text{(in general)}. \tag{83}$$

See Sec. IV.B for a general discussion on conditional entropies. Moreover, the quantum collision entropy is a measure for how mixed the state ρ_A is and defined as

$$H_{\text{coll}}(\rho_A) \coloneqq -\log \text{tr}[\rho_A^2]. \tag{84}$$

We emphasize that since Eq. (82) is an equality it is tight for every state. By the concavity of the logarithm we also have, in analogy to the Shannon entropy (77),

$$H_{\text{coll}}(K|\Theta) \leq \frac{1}{d+1}\sum_{j=1}^{d+1} H_{\text{coll}}(K|\Theta=\theta_j). \tag{85}$$

Example 14. For the qubit Pauli measurements, Eq. (82) yields $H_{\mathrm{coll}}(K|\Theta) = \log 3 - \log\left(2^{-H_{\mathrm{coll}}(\rho_A)} + 1\right)$ with $\Theta \in \{\sigma_{\mathbb{X}}, \sigma_{\mathbb{Y}}, \sigma_{\mathbb{Z}}\}$.

The uncertainty relation (81) for the Shannon entropy follows from Eq. (82) by at first only considering pure states, i.e., states with $H_{\mathrm{coll}}(\rho_A) = 0$, and using the fact that the Rényi entropies are monotonically decreasing as a function of the parameter α (note that the collision entropy corresponds to $\alpha = 2$ and the Shannon entropy to $\alpha = 1$). For mixed states ρ_A we can extend this in a second step by taking the eigendecomposition and making use of the concavity of the Shannon entropy. For later purposes we note that it is technically often accessible to work with the collision entropy H_{coll} (even when ultimately interested in uncertainty relations in terms of other entropies).

The uncertainty relation (81) was improved for d even to (Sánchez-Ruiz, 1995)

$$H(K|\Theta) \geq \frac{1}{d+1}\left[\frac{d}{2}\log\left(\frac{d}{2}\right) + \left(\frac{d}{2}+1\right)\log\left(\frac{d}{2}+1\right)\right] \quad \text{with} \quad \Theta \in \{\theta_1, \ldots, \theta_{d+1}\}. \tag{86}$$

Note that this relation generalizes the qubit result in Eq. (79) to arbitrary dimensions.

Furthermore, the uncertainty relations for a full set of $L = d+1$ MUBs can also be expressed in terms of the extrema of Wigner functions (Wootters and Sussman, 2007; Mandayam, Wehner, and Balachandran, 2010).

3. General sets of MUBs

At first glance, one might think that measuring in mutually unbiased bases always results in a large amount of uncertainty. Somewhat surprisingly, this is not the case. In fact, Ballester and Wehner (2007) showed that for $d = p^{2l}$ with p prime and $l \in \mathbb{N}$, there exist up to $L = p^l + 1$ many MUBs together with a state ρ_A for which

$$H(K|\Theta) = \frac{\log d}{2} \quad \text{with} \quad \Theta \in \{\theta_1, \ldots, \theta_L\}. \tag{87}$$

That is, we observe no more uncertainty than if we had just considered two incompatible measurements. While a certain amount of mutual unbiasedness is therefore a necessary condition for strong uncertainty relations, it is in general not sufficient.

For smaller sets of $L < d+1$ MUBs we immediately get a weak bound from an iterative application of the Maassen-Uffink relation (31) for MUBs,

$$H(K|\Theta) \geq \frac{\log d}{2} \quad \text{with} \quad \Theta \in \{\theta_1, \ldots, \theta_L\}. \tag{88}$$

It turns out that the bound (88) cannot be improved much in general, as the following example shows.

Example 15. In $d = 3$, Wehner and Winter (2010) showed that there exists a set of $L = 3$ MUBs together with a state ρ_A such that $H(K|\Theta) = 1$ for $\Theta \in \{\theta_1, \theta_2, \theta_3\}$. This allows only a relatively weak uncertainty relation. Wu, Yu, and Molmer (2009) showed that

$$H(K|\Theta) \geq \tfrac{8}{9} \approx 0.89 \quad \text{with} \quad \Theta \in \{\theta_1, \theta_2, \theta_3\}. \tag{89}$$

This is slightly stronger than the lower bound from Eq. (88):

$$H(K|\Theta) \geq \frac{\log 3}{2} \approx 0.79 \quad \text{with} \quad \Theta \in \{\theta_1, \theta_2, \theta_3\}. \tag{90}$$

Generally this allows only relatively weak uncertainty relations if $L < d+1$. Wu, Yu, and Molmer (2009) showed that

$$H_{\mathrm{coll}}(K|\Theta) \geq -\log\frac{d \cdot 2^{-H_{\mathrm{coll}}(\rho_A)} + L - 1}{L \cdot d} \quad \text{with} \quad \Theta \in \{\theta_1, \ldots, \theta_L\}. \tag{91}$$

This implies, in particular, the Shannon entropy relation (Azarchs, 2004),

$$H(K|\Theta) \geq -\log\frac{d+L-1}{L \cdot d} \quad \text{with} \quad \Theta \in \{\theta_1, \ldots, \theta_L\}, \tag{92}$$

see also Wehner and Winter (2010) for an elementary proof. For comparison, with $L = d = 3$, Eq. (92) yields

$$H(K|\Theta) \geq \log\tfrac{9}{5} \approx 0.85 \quad \text{with} \quad \Theta \in \{\theta_1, \theta_2, \theta_3\}, \tag{93}$$

which is between Eqs. (88) and (89). Additional evidence that general sets of less than $d+1$ MUBs in dimension d only generate weak uncertainty relations has been given by DiVincenzo *et al.* (2004), Ballester and Wehner (2007), and Ambainis (2010). Many of the findings also extend to the setting of approximate mutually unbiased bases (Hayden *et al.*, 2004).

In terms of the min-entropy, Mandayam, Wehner, and Balachandran (2010) showed that for measurements in L possible MUBs the following two bounds hold:

$$\frac{1}{L}\sum_{\theta=1}^{L} H_{\min}(K|\Theta=\theta) \geq -\log\left[\frac{1}{d}\left(1 + \frac{d-1}{\sqrt{L}}\right)\right], \tag{94}$$

$$\frac{1}{L}\sum_{\theta=1}^{L} H_{\min}(K|\Theta=\theta) \geq -\log\left[\frac{1}{L}\left(1 + \frac{L-1}{\sqrt{d}}\right)\right]. \tag{95}$$

Each of these is better in certain regimes, and the latter can indeed be tight. They also study uncertainty relations for certain classes of MUBs that exhibit special symmetry properties. It remains an interesting topic to study uncertainty relations for MUBs and in Sec. III.G.8 we present some related results of Kalev and Gour (2014).

4. Measurements in random bases

Another candidate for strong uncertainty relations is sets of measurements that are chosen at random.[8] Extending on the previous results of Hayden *et al.* (2004), Fawzi, Hayden, and

[8] By "at random" we mean according to the Haar measure on the unitary group; see, e.g., Hayden *et al.* (2004) for more details.

Sen (2011) show that in dimension d there exist any number of $L > 2$ measurements and a universal constant C (independent of d and L) such that

$$H(K|\Theta) \geq \log d \cdot \left(1 - \sqrt{\frac{1}{L} \cdot C \log(L)}\right) - g(L) \quad \text{with} \quad \Theta \in \{\theta_1, \ldots, \theta_L\}, \tag{96}$$

with the correction term $g(L) = O(\log[L/\log(L)])$. Note that for any set of L measurements there exists a state such that

$$H(K|\Theta) \leq \log d \cdot \left(1 - \frac{1}{L}\right) \quad \text{with} \quad \Theta \in \{\theta_1, \ldots, \theta_L\}. \tag{97}$$

Hence, Eq. (96) is already reasonably strong. However, very recently Eq. (96) was improved by proving a conjecture stated by Wehner and Winter (2010). Namely, Adamczak *et al.* (2016) showed that in dimension d there exist any number of $L > 2$ measurements and a universal constant D (independent of d and L) such that

$$H(K|\Theta) \geq \log d \cdot \left(1 - \frac{1}{L}\right) - D \quad \text{with} \quad \Theta \in \{\theta_1, \ldots, \theta_L\}. \tag{98}$$

We emphasize that this matches the upper bound (97) up to the constant D.

The downside with Eqs. (96) and (98), however, is that the measurements are not explicit. This is an issue for applications. In particular, it is computationally inefficient to sample from the Haar measure. Fawzi, Hayden, and Sen (2011) showed that the measurements in their Eq. (96) can be made explicit and efficient if the number L of measurements is small enough. More precisely, for n qubits (with n sufficiently large) and $\varepsilon > 0$, there exists a constant C and a set of

$$L \leq (n/\varepsilon)^{C \log(1/\varepsilon)} \tag{99}$$

measurements generated by unitaries computable by quantum circuits of size $O(\text{polylog}n)$ such that

$$H(K|\Theta) \geq n \cdot (1 - 2\varepsilon) - h_{\text{bin}}(\varepsilon) \quad \text{with} \quad \Theta \in \{\theta_1, \ldots, \theta_L\}, \tag{100}$$

where h_{bin} denotes the binary entropy. Equation (100) will be the basis for the information locking schemes presented in Sec. VI.H.3.

5. Product measurements on multiple qubits

For applications in cryptography we usually need uncertainty relations for measurements that can be implemented locally, so-called product measurements. For example, for an n-qubit state we are interested in uncertainty relations for the set of 2^n different measurements given by measuring each qubit independently in one of the two Pauli bases $\sigma_{\mathbb{X}}$ or $\sigma_{\mathbb{Z}}$. These are often called BB84 measurements due to the work of Bennett and Brassard (1984). Using the Maassen-Uffink bound (31) for two measurements iteratively we immediately find

$$H(K^n|\Theta^n) \geq n \cdot \tfrac{1}{2} \quad \text{with} \quad \Theta^n \in \{\theta_1, \ldots, \theta_{2^n}\}. \tag{101}$$

This relation is already tight since there exist states that achieve equality.

For cryptographic applications, the relevant measure is often not the Shannon entropy but the min-entropy. The one qubit relation (72) is easily extended to n qubits as

$$H_{\min}(K^n|\Theta^n) \geq -n \cdot \log\left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right) \approx n \cdot 0.22 \quad \text{with} \quad \Theta^n \in \{\theta_1, \ldots, \theta_{2^n}\}. \tag{102}$$

Again there exist states that achieve equality. More generally Ng, Berta, and Wehner (2012) found for n qubit BB84 measurements and the Rényi entropy of order $\alpha \in (1, 2]$,

$$H_\alpha(K^n|\Theta^n) \geq n \cdot \frac{\alpha - \log(1 + 2^{\alpha-1})}{\alpha - 1} \quad \text{with} \quad \Theta^n \in \{\theta_1, \ldots, \theta_{2^n}\}, \tag{103}$$

where the conditioning is given as (see Appendix C)[9]

$$H_\alpha(K|\Theta) = \frac{\alpha}{1-\alpha} \log\left(\frac{1}{L}\sum_{j=1}^{L} 2^{(1-\alpha)/\alpha H_\alpha(K|\Theta=\theta_j)}\right). \tag{104}$$

Similarly, it can be shown for the set of 3^n different measurements given by measuring each qubit independently in one of the three Pauli bases $\sigma_{\mathbb{X}}$, $\sigma_{\mathbb{Y}}$, or $\sigma_{\mathbb{Z}}$ that

$$H(K^n|\Theta^n) \geq n \cdot \tfrac{2}{3} \quad \text{with} \quad \Theta^n \in \{\theta_1, \ldots, \theta_{3^n}\}. \tag{105}$$

Following Bruß (1998) these measurements are often called six-state measurements. The uncertainty relation (105) is the extension of Eq. (79) from 1 to n qubits. More general relations in terms of Rényi entropies were again derived by Ng, Berta, and Wehner (2012).

Approximate extensions of all these relations when the measurements are not exactly given by the Pauli measurements $\{\sigma_{\mathbb{X}}, \sigma_{\mathbb{Y}}, \sigma_{\mathbb{Z}}\}$ have been discussed by Kaniewski, Tomamichel, and Wehner (2014). Some extensions of the n qubit relations previously discussed will be crucial for applications in two-party cryptography (Sec. VI.C).

6. General sets of measurements

Liu, Mu, and Fan (2015) gave entropic uncertainty relations for general sets of measurements. Their bounds are qualitatively different than just combining Eq. (31) iteratively and sometimes become strictly stronger in dimension $d > 2$. For simplicity we state only the case of $L = 3$ measurements (in any dimension $d \geq 2$),

[9]We emphasize that unlike in the unconditional case $H_2(K|\Theta) \neq H_{\text{coll}}(K|\Theta)$ and hence Eq. (83) is different from Eq. (104) for $\alpha = 2$.

$$H(K|\Theta) \geq \frac{1}{3}\log\frac{1}{m} + \frac{2}{3}H(\rho_A) \quad \text{with} \quad \Theta \in \{V^{(1)}, V^{(2)}, V^{(3)}\}, \tag{106}$$

and the multiple overlap constant

$$m := \max_k \left(\sum_j \max_i \left[c(v_i^1, v_j^2) \right] \cdot c(v_j^2, v_k^3) \right), \tag{107}$$

and $\{|v_i^1\rangle\}$, $\{|v_j^2\rangle\}$, and $\{|v_k^3\rangle\}$ are the eigenvectors of $V^{(1)}$, $V^{(2)}$, and $V^{(3)}$, respectively.

Example 16. For a qubit and the full set of three MUBs given by the Pauli measurements this gives

$$H(K|\Theta) \geq \tfrac{1}{3} + \tfrac{2}{3}H(\rho_A) \quad \text{with} \quad \Theta \in \{\sigma_\mathbb{X}, \sigma_\mathbb{Y}, \sigma_\mathbb{Z}\}. \tag{108}$$

This bound is, however, weaker than Eqs. (78) and (80). On the other hand, of course the whole point of the bound (106) is that in contrast to Eqs. (78) and (80) it can be applied to any set of $L = 3$ measurements (in arbitrary dimension).

See Liu, Mu, and Fan (2015) for a fully worked out example where their bound can become stronger than any bounds implied by two measurement relations.

7. Anticommuting measurements

As already noted in Sec. III.D, many interesting measurements are not of the orthonormal basis form, but are more generally described by POVMs. One class of such measurements that generate maximally strong uncertainty relations are sets of anticommuting POVMs with only two possible measurement outcomes. In more detail, we consider a set $\{\mathbb{X}_1, \ldots, \mathbb{X}_L\}$ of binary POVMs $\mathbb{X}_j = \{\mathbb{X}_j^0, \mathbb{X}_j^1\}$ that generate binary observables

$$O_j := \mathbb{X}_j^0 - \mathbb{X}_j^1 \quad \text{with} \quad [O_j, O_k]_+ = 2\delta_{jk}, \tag{109}$$

where, as in Eq. (59), $[\cdot,\cdot]_+$ denotes the anticommutator.[10] The goal is then to find lower bounds on entropies of the form $H(K|\Theta)$ with

$$P_{K\Theta}(k, \mathbb{X}_j) := \frac{1}{L}\mathrm{tr}[\mathbb{X}_j^k \rho_A] \quad \text{with} \quad k \in \{0,1\}, \; j \in \{1, \ldots, L\}. \tag{110}$$

For simplicity we discuss only the case of n qubit states for which we have sets of up to $2n+1$ many binary anticommuting POVMs.[11] Wehner and Winter (2008) then showed that

$$H(K|\Theta) \geq 1 - \frac{1}{L} \quad \text{with} \quad k \in \{0,1\} \tag{111}$$

for any subset $\Theta \subseteq \{\mathbb{X}_1, \ldots, \mathbb{X}_{2n+1}\}$ of size L. These relations are tight and reduce for the $L = 3$ qubit Pauli measurements $\{\sigma_\mathbb{X}, \sigma_\mathbb{Y}, \sigma_\mathbb{Z}\}$ to the bound (79). Similarly Wehner and Winter (2008) also found for the collision entropy

$$\frac{1}{L}\sum_{\mathbb{X}_j \in \Theta} H_{\mathrm{coll}}(K|\Theta = \mathbb{X}_j) \geq 1 - \log\left(1 + \frac{1}{L}\right), \tag{112}$$

and the min-entropy

$$\frac{1}{L}\sum_{\mathbb{X}_j \in \Theta} H_{\min}(K|\Theta = \mathbb{X}_j) \geq 1 - \log\left(1 + \frac{1}{\sqrt{L}}\right). \tag{113}$$

These relations are again tight. Note, however, that the average over the basis choice is outside of the logarithm, whereas for the collision and the min-entropy the average is more naturally inside of the logarithm as, e.g., in Eqs. (82) and (102).

Example 17. For the $L = 3$ qubit case Eq. (112) reduces to

$$\frac{1}{3}\sum_{j=X,Y,Z} H_{\mathrm{coll}}(K|\Theta = \sigma_j) \geq \log 3 - 1, \tag{114}$$

which, as seen by Eq. (85), is generally weaker than the corresponding bound implied by (82),

$$H_{\mathrm{coll}}(K|\Theta) \geq \log 3 - 1 \quad \text{with} \quad \Theta \in \{\sigma_\mathbb{X}, \sigma_\mathbb{Y}, \sigma_\mathbb{Z}\}. \tag{115}$$

Finally, see Ver Steeg and Wehner (2009) for the connection of the uncertainty relations described in this section to Bell inequalities.

8. Mutually unbiased measurements

In Sec. III.G.2 we discussed how full sets of $d+1$ MUBs give rise to strong uncertainty relations; see, e.g., Eq. (81). However, for general dimension d we do not know if a full set of $d+1$ MUBs always exists (see Appendix A for a discussion). Kalev and Gour (2014) offered the following generalization of MUBs to measurements that are not necessarily given by a basis. Two POVMs $\mathbb{X} = \{\mathbb{X}^x\}_{x=1}^d$ and $\mathbb{Z} = \{\mathbb{Z}^z\}_{z=1}^d$ on a d-dimensional quantum system are mutually unbiased measurements (MUMs) if, for some $\kappa \in (1/d, 1]$,

$$\mathrm{tr}[\mathbb{X}^x] = 1, \quad \mathrm{tr}[\mathbb{Z}^z] = 1, \quad \mathrm{tr}[\mathbb{X}^x\mathbb{Z}^z] = \frac{1}{d} \;\; \forall\, x, z, \tag{116}$$

$$\mathrm{tr}[\mathbb{X}^x\mathbb{X}^{x'}] = \delta_{xx'}\cdot\kappa + (1-\delta_{xx'})\frac{1-\kappa}{d-1} \quad \forall\, x, x', \tag{117}$$

and similarly for z, z'. In addition, a set of POVMs $\{\mathbb{X}_1, \ldots, \mathbb{X}_n\}$ is called a set of MUMs if each POVM $\mathbb{X}_j$ is mutually unbiased to each other POVM $\mathbb{X}_k$, with $k \neq j$, in the set.

[10] An example of such anticommuting sets in the case of $L = 3$ is provided by the qubit Pauli operators $\{\sigma_\mathbb{X}, \sigma_\mathbb{Y}, \sigma_\mathbb{Z}\}$.

[11] This is obtained by the unique Hermitian representation of the Clifford algebra via the Jordan-Wigner transformation (Dietz, 2006).

A straightforward example is again MUBs for which $\kappa = 1$.[12] The crucial observation of Kalev and Gour (2014) is that in any dimension d a full set of $d+1$ MUMs exists (see their paper for the explicit construction). Moreover, every full set of $d+1$ MUMs gives rise to a strong uncertainty relation,

$$H(K|\Theta) \geq \log(d+1) - \log(1+\kappa) \tag{118}$$

with $\Theta \in \{\mathbb{X}_1, \ldots, \mathbb{X}_{d+1}\}$, where the notation is as introduced in Eq. (110). This is in full analogy with Eq. (81) for a full set of $d+1$ MUBs. Tighter and state-dependent versions of Eq. (118) as well as extensions to Rényi entropies can be found in Chen and Fei (2015) and Rastegin (2015b).

H. Fine-grained uncertainty relations

So far we have expressed uncertainty in terms of the von Neumann entropy and the Rényi entropies of the probability distribution induced by the measurement. Recall, however, that any restriction on the set of allowed probability distributions over measurement outcomes can be understood as an uncertainty relation, and hence there are many ways of formulating such restrictions. Thus, while generally the Rényi entropies determine the underlying probability distribution of the measurement outcomes uniquely,[13] it is interesting to ask whether we can formulate more refined versions of uncertainty relations.

Suppose we perform L measurements labeled Θ on a preparation ρ_A, where each measurement has N outcomes. Fine-grained uncertainty relations (Oppenheim and Wehner, 2010) consist of a set of N^L equations which state that for all states we have

$$\sum_{\theta=1}^{L} P_\Theta(\Theta=\theta) P_X(X = x_\theta|\Theta=\theta) \leq \zeta_{x_1,\ldots,x_L}, \tag{119}$$

for all combinations of measurement outcomes $x_1, \ldots, x_L$ that are possible for the L different measurements. Here $P_\Theta(\Theta=\theta)$ is the probability of choosing a measurement labeled $\Theta=\theta$ and $0 \leq \zeta_{x_1,\ldots,x_L} \leq 1$.

Note that whenever $\zeta_{x_1,\ldots,x_L} < 1$, then we observe some amount of uncertainty, since it implies that we cannot simultaneously have $P_X(X=x_\theta|\Theta=\theta)=1$ for all θ. We remark that fine-grained uncertainty relations naturally give a lower bound on the min-entropy since

$$2^{-H_{\min}(X|\Theta)} = \sum_{\theta=1}^{L} P_\Theta(\Theta=\theta) \max_{x_\theta} P_X(X=x_\theta|\Theta=\theta) \tag{120}$$

$$\leq -\log \max_{x_1,\ldots,x_L} \zeta_{x_1,\ldots,x_L}. \tag{121}$$

However, fine-grained uncertainty relations are strictly more informative and are also closely connected to Bell nonlocality (Oppenheim and Wehner, 2010). While not the topic of this survey, a number of extensions of these fine-grained uncertainty relations are known (Dey, Pramanik, and Majumdar, 2013; Ren and Fan, 2014; Rastegin, 2015a).

I. Majorization approach to entropic uncertainty

Another way to capture uncertainty relations that relate directly to entropic ones is given by the majorization approach. Instead of sums of probabilities, we look here at products. The idea to derive entropic uncertainty relations via a majorization relation was pioneered by Partovi (2011) and later extended and clarified independently by Friedland, Gheorghiu, and Gour (2013) and Puchała, Rudnicki, and Życzkowski (2013). We recall the distributions P_X and P_Z resulting from the measurements $\mathbb{X}$ and $\mathbb{Z}$, respectively, of the state ρ_A as in Eq. (48). We denote by $P_X^\downarrow$ and $P_Z^\downarrow$ the corresponding reordered vectors such that the probabilities are ordered from largest to smallest.

1. Majorization approach

The main objective of this section is to find a vector that majorizes the tensor product of the two probability vectors $P_X^\downarrow$ and $P_Z^\downarrow$. Namely, we are looking for a probability distribution $\nu = \{\nu(1), \nu(2), \ldots, \nu(|X||Z|)\}$ such that[14]

$$P_X^\downarrow \times P_Z^\downarrow \prec \nu \quad \text{holds for all} \quad \rho \in \mathcal{S}(\mathcal{H}). \tag{122}$$

Such a relation gives a bound on how spread out the product distribution $P_X^\downarrow \times P_Z^\downarrow$ must be. A simple and instructive example of a probability distribution ν satisfying Eq. (122) can be constructed as follows. Consider the largest probability in the product distribution in Eq. (122), given by

$$p_1 := P_X^\downarrow(1) \cdot P_Z^\downarrow(1) = p_{\text{guess}}(X) \cdot p_{\text{guess}}(Z). \tag{123}$$

We know that p_1 is always bounded away from 1 if the two measurements are incompatible, since it cannot be that both measurements have a deterministic outcome. For example, recall that we have Eq. (68) from Deutsch (1983), which gives

$$p_1 = p_{\text{guess}}(X) \cdot p_{\text{guess}}(Z) \leq b^2 =: \nu_1, \tag{124}$$

where b was defined in Eq. (40). As such, it is immediately clear that the vector $\nu^1 = \{\nu_1, 1-\nu_1, 0, \ldots, 0\}$ satisfies Eq. (122) and in fact constitutes a simple but nontrivial uncertainty relation.

Going beyond this observation, the works of Friedland, Gheorghiu, and Gour (2013) and Puchała, Rudnicki, and Życzkowski (2013) both present an explicit method to construct a sequence of vectors $\{\nu^k\}_{k=1}^{|X|-1}$ of the form

[12] The trivial example for which each POVM element is the maximally mixed state $\mathbb{1}/d$ is excluded because this would correspond to $\kappa = 1/d$.

[13] To see this, note that the cumulant generating function of the random variable $Z = -\log P_X(X)$ can be expressed in terms of the Rényi entropy of X, namely, $g_Z(s) = H_{1+s}(X)$. The cumulants of Z and hence the distributions of Z and X are thus fully determined by the Rényi entropy in a neighborhood around $\alpha = 1$.

[14] Recall the definition of majorization in Sec. III.A.3.

$$\nu^k = \{\nu_1, \nu_2 - \nu_1, \ldots, 1 - \nu_{k-1}, 0, \ldots, 0\}, \tag{125}$$

with $\nu^k \prec \nu^{k-1}$ that satisfy Eq. (122) and lead to tighter and tighter uncertainty relations. The expressions for ν_k are given in terms of an optimization problem and become gradually more difficult as k increases. See these papers for details on the construction.

2. From majorization to entropy

Entropic uncertainty relations for Rényi entropy follow directly from the majorization relation due to the fact that the Rényi entropy is Schur concave and additive. This implies that

$$P_X^{\downarrow} \times P_Z^{\downarrow} \prec \nu \Rightarrow H_\alpha(X) + H_\alpha(Z) \geq H_\alpha(V), \tag{126}$$

where V is a random variable distributed according to the law ν. These uncertainty relations have a different flavor than the Maassen-Uffink relations in Eq. (35) since they provide a bound on the sum of the Rényi entropy of the same parameter. As a particular special case for $\alpha = \infty$, we get back Deutsch's uncertainty relation (Deutsch, 1983),

$$H(X) + H(Z) \geq H_{\min}(X) + H_{\min}(Z) \tag{127}$$

$$\geq -2 \log b =: q_{\mathrm{D}}, \tag{128}$$

where the first inequality follows by the monotonicity of the Rényi entropy in the parameter α. However, an immediate improvement on this relation can be obtained by applying Eq. (126) directly for $\alpha = 1$, which yields

$$H(X) + H(Z) \geq h_{\mathrm{bin}}(b^2) =: q_{\mathrm{maj}}. \tag{129}$$

See Fig. 6 for a comparison of this to other bounds.

3. Measurements in random bases

An interesting special case for which a majorization-based approach gives tighter bounds is for measurements in two bases $\mathbb{X}$ and $\mathbb{Z}$ related by a random unitary. Intuitively, we would expect such bases to be complementary. More precisely, for any measurement in a fixed basis $\mathbb{X}$ and $\mathbb{Z}$ related by a unitary drawn from the Haar measure on the unitary group, Adamczak *et al.* (2016) showed that for the Masseen-Uffink bound (31) we have with probability going to 1 for $d \to \infty$,

$$H(X) + H(Z) \geq \log d - \log \log d. \tag{130}$$

However, they also show that a majorization-based approach yields the tighter estimate

$$H(X) + H(Z) \geq \log d - C_1, \tag{131}$$

where $C_1 > 0$ is some constant. This is close to optimal since we have that with probability going to 1 for $d \to \infty$ (Adamczak *et al.*, 2016),

$$\log d - C_0 \geq H(X) + H(Z), \tag{132}$$

for some constant $C_0 > 0$. It is an open question to determine the exact asymptotic behavior, i.e., the constant $C \in (C_0, C_1)$ that gives a lower and an upper bound.

4. Extensions

The majorization approach has also been extended to cover general POVMs and more than two measurements (Friedland, Gheorghiu, and Gour, 2013; Rastegin and Życzkowski, 2016). Moreover, Rudnicki, Puchała, and Życzkowski (2014) discussed a related method, based on finding a vector that majorizes the ordered distribution $(P_X \cup P_Z)^{\downarrow}$, where $P_X \cup P_Z$ is simply the concatenation of the two probability vectors. This yields a further improvement on Eq. (129). Finally, an extension to uncertainty measures that are not necessarily Schur concave but only monotonic under doubly stochastic matrices was presented by Narasimhachar, Poostindouz, and Gour (2016).

IV. UNCERTAINTY GIVEN A MEMORY SYSTEM

The uncertainty relations presented thus far are limited in the following sense: they do not allow the observer to have access to side information. Side information, also known as memory, might help the observer to better predict the outcomes of the $\mathbb{X}$ and $\mathbb{Z}$ measurements. It is therefore a fundamental question to ask: does the uncertainty principle still hold when the observer has access to a memory system? If so, what form does it take?

The uncertainty principle in the presence of memory is important for cryptographic applications and witnessing entanglement (Sec. VI). For example, in quantum key distribution, an eavesdropper may gather some information, store it in her memory, and then later use that memory to try to guess the secret key. It is crucial to understand whether the eavesdropper's memory allows her to break a protocol's security, or whether security is maintained. This is where general uncertainty relations that allow for memory are needed.

Furthermore, such uncertainty relations are also important for basic physics. For example, the quantum-to-classical transition is an area of physics where one tries to understand why and how quantum interference effects disappear on the macroscopic scale. This is often attributed to decoherence, where information about the system of interest S flows out to an environment E (Zurek, 2003). In decoherence, it is important to quantify the trade-off between the flow of one kind of information, say $\mathbb{Z}$, to the environment versus the preservation of another kind of information, say $\mathbb{X}$, within the system S. Here one associates $\mathbb{X}$ with the "phase" information that is responsible for quantum interference. Hence, one can see how this ties back into the quantum-to-classical transition, since loss of $\mathbb{X}$ information would destroy the quantum interference pattern. In this discussion, system E plays the role of the memory, and hence uncertainty relations that allow for memory are essentially uncertainty relations that allow the system to interact with an environment. We discuss this more in Sec. VI.F, in the context of interferometry experiments.

A. Classical versus quantum memory

With this motivation in mind, we now consider two different types of memories. First we discuss the notion of a *classical memory*, i.e., a system B that has no more than classical correlations with the system A that is to be measured.

Example 18. Consider a spin-1/2 particle A and a (macroscopic) coin B as depicted in Fig. 7(a). Suppose that we flip the coin to determine whether or not we prepare A in the spin-up state $|0\rangle$ or the spin-down state $|1\rangle$. Denoting the basis $\mathbb{Z} = \{|0\rangle, |1\rangle\}$ we see that B is perfectly correlated to this basis. That is, before the measurement of A the joint state is

$$\rho_{AB} = \tfrac{1}{2}(|0\rangle\langle 0|_A \otimes \rho_B^0 + |1\rangle\langle 1|_A \otimes \rho_B^1), \tag{133}$$

where $\mathrm{tr}[\rho_B^0 \rho_B^1] = 0$. Hence, if the observer has access to B then he can perfectly predict the outcome of the $\mathbb{Z}$ measurement on A. On the other hand, if we keep B hidden from the observer, then he can only guess the outcome of the $\mathbb{Z}$ measurement on A with probability 1/2.

We conclude from example 18 that indeed having access to B reduces the uncertainty about $\mathbb{Z}$. However, notice that a classical memory B provides no help to the observer if he tries to guess the outcome of a measurement on A that is complementary to $\mathbb{Z}$. Consider now a more general memory, one that can have any kind of correlations with system A allowed by quantum mechanics. This is called a *quantum memory* or *quantum side information* (and includes classical memory as a special case). We remark that quantum memories are becoming an experimental reality [see, e.g., Julsgaard *et al.* (2004)].

Example 19. Consider two spin-1/2 particles A and B that are maximally entangled, say in the state

$$|\psi\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB}). \tag{134}$$

This is depicted in Fig. 7(b). As with the classical memory in example 18, giving the observer access to B allows him to perfectly predict the outcome of a $\mathbb{Z}$ measurement on A (by just measuring the $\mathbb{Z}$ observable on B). But in contrast to the case with classical memory, B can also be used to predict the outcome of a complementary measurement $\mathbb{X} = \{|+\rangle, |-\rangle\}$, with $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$ on A. This follows by rewriting the maximally entangled state (134) as

$$|\psi\rangle_{AB} = \frac{1}{\sqrt{2}}(|++\rangle_{AB} + |--\rangle_{AB}), \tag{135}$$

which implies that the observer can simply measure the $\mathbb{X}$ basis on B to guess $\mathbb{X}$ on A.

The idea described in example 19 dates back to the famous EPR paper (Einstein, Podolsky, and Rosen, 1935) and raises the question of whether we can still find nontrivial bounds on the uncertainty of complementary measurements when conditioning on quantum memory. In the rest of Sec. IV we analyze this interplay between uncertainty and quantum correlations quantitatively and present entropic uncertainty relations that allow the observer to have access to (quantum) memory. For that we first introduce measures of *conditional entropy*.

(a) Illustration showing an electron spin whose $\mathbb{Z}$ component is correlated to a classical coin.

(b) Illustration showing an electron spin whose $\mathbb{Z}$ and $\mathbb{X}$ components are respectively correlated to the $\mathbb{Z}$ and $\mathbb{X}$ components of another electron spin, i.e., a quantum memory.

FIG. 7. Comparison of classical and quantum memory.

B. Background: Conditional entropies

1. Classical-quantum states

Our main goal here is to describe the entropy of a measured (and thus classical) random variable from the perspective of an observer who possesses a quantum memory. For this purpose, consider a classical register correlated with a quantum memory, modeled by a joint classical-quantum state

$$\rho_{XB} = \sum_x P_X(x)|x\rangle\langle x|_X \otimes \rho_B^x. \tag{136}$$

Here ρ_B^x is the quantum state of the memory system B conditioned on the event $X = x$. Formally, quantum states or density operators are positive semidefinite operators with unit trace acting on the Hilbert space B. In order to represent the joint system XB in the density operator formalism we also introduced an auxiliary Hilbert space X with fixed orthonormal basis $\{|x\rangle_X\}_x$.

2. Classical-quantum entropies

The interpretation of the min-entropy from Eq. (17) in terms of the optimal guessing probability gives a natural means to generalize the min-entropy to the setting with quantum memory. Clearly, an observer with access to the quantum memory B can measure out B to improve his guess. The optimal guessing probability for such an observer is then given by the optimization problem

$$p_{\mathrm{guess}}(X|B) := \max_{\mathbb{X}_B} \sum_x P_X(x)\mathrm{tr}[\mathbb{X}_B^x \rho_B^x], \tag{137}$$

where $\mathbb{X}_B$ is a POVM on B. Consequently, the conditional min-entropy is defined as (Renner, 2005; König, Renner, and Schaffner, 2009)

$$H_{\min}(X|B) := -\log p_{\mathrm{guess}}(X|B). \tag{138}$$

This is our first measure of conditional entropy. It quantifies the uncertainty of the classical register X from the perspective of an observer with access to the quantum memory (or side information) B. The more difficult it is to guess the value of X, the smaller is the guessing probability and the higher is the conditional min-entropy.

The collision entropy from Eq. (16) can likewise be interpreted in terms of a guessing probability. Consider the following generalization of the collision entropy to the case where the observer has a quantum memory B (Buhrman *et al.*, 2008):

$$H_{\mathrm{coll}}(X|B) := -\log p^{\mathrm{pg}}_{\mathrm{guess}}(X|B). \tag{139}$$

Here the pretty good guessing probability is given by

$$p^{\mathrm{pg}}_{\mathrm{guess}}(X|B) := \sum_x P_X(x)\mathrm{tr}[\Pi^x_B \rho^x_B], \tag{140}$$

where $\Pi^x_B = P_X(x)\rho_B^{-1/2}\rho^x_B\rho_B^{-1/2}$. The Π^x_B are POVM elements corresponding to the so-called pretty good measurement. The name is due to the fact that this measurement is close to optimal, in the sense that (Hausladen and Wootters, 1994)

$$p^2_{\mathrm{guess}}(X|B) \le p^{\mathrm{pg}}_{\mathrm{guess}}(X|B) \le p_{\mathrm{guess}}(X|B). \tag{141}$$

That is, if the optimal guessing probability is close to 1, then so is the pretty good guessing probability. Hence, $H_{\mathrm{coll}}(X|B)$ quantifies how well Bob can guess X given that he performs the pretty good measurement on B. In particular this also implies that

$$H_{\min}(X|B) \le H_{\mathrm{coll}}(X|B) \le 2H_{\min}(X|B). \tag{142}$$

Finally, consider the Shannon entropy $H(X)$, whose quantum counterpart $H(\rho)$ is the von Neumann entropy as defined in Eq. (45). The von Neumann entropy of X conditioned on a quantum memory B is defined as

$$H(X|B) := H(\rho_{XB}) - H(\rho_B), \tag{143}$$

where ρ_{XB} is given by Eq. (136), and

$$\rho_B = \mathrm{tr}_X[\rho_{XB}] = \sum_x P_X(x)\rho^x_B. \tag{144}$$

Although $H(X|B)$ does not have a direct interpretation as a guessing probability, it does have an operational meaning in information theory. For example, if Alice samples from the distribution P_X and Bob possesses system B, then $H(X|B)$ is the minimal information that Alice must send to Bob in order for Bob to determine the value of X. [More precisely, $H(X|B)$ is the minimal rate in bits per copy that Alice must send to Bob in the asymptotic limit of many copies of the state ρ_{XB} (Devetak and Winter, 2003).]

3. Quantum entropies

The classical-quantum conditional entropy is merely a special case of the quantum conditional entropy. It is useful to introduce the latter here, since the quantum conditional entropy will play an important role in the following.

In the simplest case, the von Neumann conditional entropy of an arbitrary bipartite state ρ_{AB} with $\rho_B = \mathrm{tr}_A(\rho_{AB})$ takes the form

$$H(A|B) := H(\rho_{AB}) - H(\rho_B). \tag{145}$$

We remark that, in general, fully quantum conditional entropy can be negative.[15] This is a signature of entanglement. In fact, the quantity $-H(A|B)$, commonly known as coherent information, provides a lower bound on the distillable entanglement (Devetak and Winter, 2005). We discuss this connection further around Eq. (330).

The fully quantum min-entropy also has a connection to entanglement. Namely, it can be written as

$$H_{\min}(A|B) := -\log[d_A \cdot F(A|B)], \tag{146}$$

where

$$F(A|B) := \max_{\mathcal{E}:B\to A'} F\big((\mathcal{I}\otimes\mathcal{E})(\rho_{AB}), |\phi_{AA'}\rangle\langle\phi_{AA'}|\big) \tag{147}$$

with the fidelity

$$F(\rho,\sigma) := \left(\mathrm{tr}\left[\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}\right]\right)^2$$

from (Uhlmann, 1985). Here $|\phi_{AA'}\rangle$ is a maximally entangled state of dimension $|A|$, and the maximization over all quantum channels $\mathcal{E}$ that map B to A'. One can think of $F(A|B)$ as the recoverable entanglement fidelity. In that sense, $-H_{\min}(A|B)$ quantifies how close the state is to a maximally entangled state.

The fully quantum collision entropy can also be related to a recoverable entanglement fidelity in close analogy to the earlier discussion for the classical-quantum case. Namely, we have (Berta, Coles, and Wehner, 2014)

$$H_{\mathrm{coll}}(A|B) := -\log[d_A \cdot F^{\mathrm{pg}}(A|B)], \tag{148}$$

where

$$F^{\mathrm{pg}}(A|B) := F\big((\mathcal{I}\otimes\mathcal{E}^{\mathrm{pg}})(\rho_{AB}), |\phi_{AA'}\rangle\langle\phi_{AA'}|\big). \tag{149}$$

Here $\mathcal{E}^{\mathrm{pg}}$ is the pretty good recovery map, whose action on an operator O is given by

$$\mathcal{E}^{\mathrm{pg}}(O) = \big(\mathrm{tr}_B[(\mathbb{1}\otimes\rho_B^{-1/2}O\rho_B^{-1/2})\rho_{A'B}]\big)^T, \tag{150}$$

where $(\cdot)^T$ denotes the transpose map, and $\rho_{A'B} = \rho_{AB}$, with system A' being isomorphic to system A.[16] In analogy to

[15] This should not concern us further here; a consistent interpretation of negative entropies is possible in the context of quantum information processing (Horodecki, Oppenheim, and Winter, 2006) and also in thermodynamics (del Rio *et al.*, 2011).

[16] One can verify that $\mathcal{E}^{\mathrm{pg}}$ is a valid quantum operation because it is a completely positive and trace-preserving map (assuming ρ_B is full rank).

Eq. (141), the pretty good recovery map is close to optimal (Barnum and Knill, 2002),

$$F^2(A|B) \leq F^{\mathrm{pg}}(A|B) \leq F(A|B). \tag{151}$$

As in the classical case, these conditional entropies emerge as special cases of Rényi entropies (Müller-Lennert *et al.*, 2013). We discuss this connection in Appendix C.

4. Properties of conditional entropy

Section III.A.3 discussed properties of entropies, which are special cases of conditional entropies with trivial conditioning systems. Here we mostly discuss properties of the conditional von Neumann entropy $H(A|B)$ and note only that similar properties also hold for other conditional entropies such as $H_{\min}(A|B)$ and $H_{\mathrm{coll}}(A|B)$ (or more generally Rényi entropies).

First, the conditional entropy reduces to the unconditional entropy for product states. That is, for bipartite states of the form $\rho_{AB} = \rho_A \otimes \rho_B$, we have $H(A|B) = H(A)$. Second, note that the entropy of a classical-quantum state is non-negative,

$$H(X|B) \geq 0 \quad \text{for } X \text{ a classical register.} \tag{152}$$

In contrast, as noted previously, the fully quantum entropy $H(A|B)$ can be negative.

A fundamental property is the so-called data-processing inequality. It says that the uncertainty of A conditioned on some system B never goes down if one processes system B, i.e., acts on B with a quantum channel $\mathcal{E}\colon B \to B'$. That is (Lieb and Ruskai, 1973),

$$H(A|B) \leq H(A|B'). \tag{153}$$

This includes the case where system $B = B_1B_2$ is bipartite and the processing corresponds to discarding a subsystem, say B_2. In this case the data-processing inequality takes the form $H(A|B) \leq H(A|B_1)$. This inequality is intuitive in the sense that having access to more information can never increase the uncertainty.

Another useful property of conditional entropies is related to the monogamy of entanglement. This corresponds to the idea that the more A is entangled with B the less A is entangled with a purifying system C. Suppose that C is a system that purifies ρ_{AB}, i.e., $\rho_{ABC} = |\psi\rangle\langle\psi|$. Then, we have

$$H(A|B) = -H(A|C). \tag{154}$$

Typically one associates entanglement with a negative conditional entropy, and indeed as discussed previously the coherent information (the negative of the conditional entropy) lower bounds the distillable entanglement. In this sense, the relation in Eq. (154) captures the intuition of monogamy of entanglement. It implies that if ρ_{AB} has a negative conditional entropy, then ρ_{AC} must have a positive conditional entropy. So there is a trade-off between the entanglement present in ρ_{AB} and in ρ_{AC}.

The relation in Eq. (154) is called the duality relation, as it relates an entropy to its *dual* entropy. As we have seen the von Neumann entropy is dual to itself but in general the duality relation involves two different entropies. For example, the min-entropy is dual to the max-entropy,

$$H_{\max}(A|B) \coloneqq -H_{\min}(A|C). \tag{155}$$

We take Eq. (155) as the definition of the max-entropy, although an explicit expression in terms of the marginal ρ_{AB} can be derived (König, Renner, and Schaffner, 2009). More generally, the duality relation for the Rényi entropy family is given in Appendix C.2.

C. Classical memory uncertainty relations

We now have all the measures at hand to discuss uncertainty relations that allow for a memory system. Naturally, we begin with the simplest case of a classical memory. It turns out that uncertainty relations that allow for classical memory are often easy to derive from the uncertainty relations without memory, particularly for the Shannon entropy (Hall, 1995). Consider the conditional Shannon entropy, which can be written as

$$H(X|Y) = H(XY) - H(Y) = \sum_y P_Y(y) H(X|Y=y). \tag{156}$$

Now consider some generic Shannon entropy uncertainty relation for measurements $\mathbb{X}^n$ and quantum states ρ_A:

$$\sum_n H(X_n) \geq q \quad \text{where } P_{X_n}(x) = \langle \mathbb{X}_n^x | \rho_A | \mathbb{X}_n^x \rangle$$
$$\text{and} \quad q > 0 \text{ state independent.} \tag{157}$$

The goal is to extend this to quantum-classical states ρ_{AY}, where the classical memory Y holds some information about the preparation of the quantum marginal

$$\rho_{AY} = \sum_y P_Y(y) \rho_A^y \otimes |y\rangle\langle y|_Y \tag{158}$$

with distributions $P_{X_nY}(x,y) = P_Y(y)\langle \mathbb{X}_n^x | \rho_A^y | \mathbb{X}_n^x \rangle$. However, assuming that the uncertainty relation (157) holds for all quantum states, it holds, in particular, for each conditional state ρ_A^y associated with $Y = y$ in the classical memory Y. Averaging over y gives

$$\sum_y P_Y(y) \sum_n H(X_n|Y=y) \geq \sum_y P_Y(y) q = q. \tag{159}$$

Hence, we find by Eq. (156) that

$$\sum_n H(X_n) \geq q \Rightarrow \sum_n H(X_n|Y) \geq q. \tag{160}$$

That is, any Shannon entropy uncertainty relation of the form (157) implies a corresponding uncertainty relation in terms of the conditional Shannon entropy of the form (160). Note that the conditional version (160) even provides a stronger bound, since by the data-processing inequality (153) conditioning on side information can only reduce uncertainty.

Example 20. Consider a bipartite state ρ_{AB}, where Alice will measure system A in one of two bases $\mathbb{X}$ or $\mathbb{Z}$ and Bob will measure system B in the basis $\mathbb{Y}$. Then, the Maassen-Uffink relation (31) implies

$$H(X|Y) + H(Z|Y) \geq q_{\mathrm{MU}}, \tag{161}$$

for the distribution

$$P_{XY}(x,y) = \langle \mathbb{X}^x \otimes \mathbb{Y}^y | \rho_{AB} | \mathbb{X}^x \otimes \mathbb{Y}^y \rangle, \tag{162}$$

and analogously $P_{ZY}(z,y)$.

It is worth noting that the classical memory Y can be considered multipartite, say, of the form $Y = Y_1 Y_2 \cdots Y_n$ (Cerf *et al.*, 2002; Renes and Boileau, 2009). Since by the data-processing inequality (153) discarding subsystems of Y can never reduce the uncertainty, Eq. (160) implies that

$$\sum_n H(X_n) \geq q \Rightarrow \sum_n H(X_n|Y_n) \geq q. \tag{163}$$

Example 21. Consider a tripartite state ρ_{ABC}, where Alice will measure system A in one of two bases $\mathbb{X}$ or $\mathbb{Z}$, Bob will measure system B in the basis $\mathbb{Y}_B$, and the third party Charlie will measure system C in the basis $\mathbb{Y}_C$. Then, the Maassen-Uffink relation (31) implies

$$H(X|Y_B) + H(Z|Y_C) \geq q_{\mathrm{MU}}. \tag{164}$$

This relation is reminiscent of the scenario in quantum key distribution. Namely, if Alice and Bob verify that $H(X|Y_B)$ is close to zero, then Eq. (164) implies that Charlie is fairly ignorant about Z. That is, $H(Z|Y_C)$ is roughly q_{MU} or larger. We emphasize, however, that Eq. (164) cannot be used to prove security against general quantum memory eavesdropping attacks (see Sec. VI.B).

D. Bipartite quantum memory uncertainty relations

1. Guessing game with quantum memory

Let us now make explicit what the guessing game (see Sec. III.F) looks like when we allow quantum memory. Specifically, the rules of the game now allow Bob to keep a quantum memory system in order to help him guess Alice's measurement outcome. This is illustrated in Fig. 8.

(1) Bob prepares a bipartite quantum system AB in a state ρ_{AB}. He sends system A to Alice while he keeps system B.
(2) Alice performs one of two possible measurements $\mathbb{X}$ or $\mathbb{Z}$ on A and stores the outcome in the classical register K. She communicates her choice to Bob.
(3) Bob's task is to guess K.

Note that in this game, Bob can make an *educated* guess based on his quantum memory B.

Example 22. Let the A system be one qubit and Alice's two measurements given by $\sigma_{\mathbb{X}}$ and $\sigma_{\mathbb{Z}}$. Then Bob can win the game with probability 1 by preparing the maximally entangled state and using the strategy from example 19.

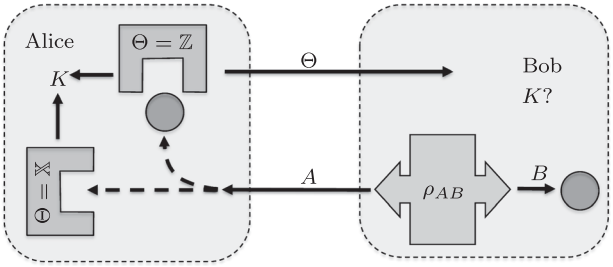


FIG. 8. The guessing game in the presence of a quantum memory system. First, Bob prepares AB in state ρ_{AB} and then sends system A to Alice. Second, Alice performs either the $\mathbb{X}$ or $\mathbb{Z}$ measurement on A and then announces the measurement choice Θ to Bob. Bob's task is to correctly guess K. The question is thus: how uncertain is Bob about Alice's measurement outcome K, given that he has access to B and Θ?

This example illustrates the power of a quantum memory, and, in particular, of one that is *entangled* with the system being measured. At first sight, this might seem to violate the usual notion of the uncertainty principle. However, it does not. What it illustrates is that the usual formulations of the uncertainty principle, such as the Robertson relation (2) or the Maassen-Uffink relation (31), are not about conditional uncertainty. Equations (2) and (31) are perfectly valid but limited in this sense.

2. Measuring in two orthonormal bases

Let us first discuss how the Maassen-Uffink relation (31) can be extended to the setup when the observer has a quantum memory. Note that examples 19 and 22 illustrate that the bound in the uncertainty relation must become trivial in the case where Bob's memory is maximally entangled to Alice's system. On the other hand, we know that the bound must be nontrivial when Bob has no memory, since this corresponds to the situation covered by Eq. (31). Likewise if Bob has a memory that is only classically correlated to Alice's system, then we already saw in Eq. (161) that the Maassen-Uffink relation can be extended. Therefore, it becomes clear that we need a state-dependent extension: a bound that becomes weaker as Bob's memory is more entangled with Alice's system. Indeed, Berta *et al.* (2010) proved the following uncertainty relation. For any bipartite state ρ_{AB} and any orthonormal bases $\mathbb{X}$ and $\mathbb{Z}$,

$$H(X|B) + H(Z|B) \geq q_{\mathrm{MU}} + H(A|B), \tag{165}$$

with q_{MU} as in Eq. (31). Here the conditional entropy $H(X|B)$ is evaluated on the classical-quantum state

$$\rho_{XB} = \sum_x |x\rangle\langle x|_X \otimes (\langle \mathbb{X}^x| \otimes \mathbb{1}_B) \rho_{AB} (|\mathbb{X}^x\rangle \otimes \mathbb{1}_B), \tag{166}$$

and similarly for $H(Z|B)$. The classical-quantum conditional entropies $H(X|B)$ and $H(Z|B)$ quantify Bob's uncertainty about X and Z, respectively, given that Bob has access to the quantum memory B.

The quantity $H(A|B)$ on the right-hand side of Eq. (165) makes the bound state dependent. We already mentioned

around Eq. (145) that $-H(A|B)$ is a quantifier of the entanglement present in ρ_{AB}. For maximally entangled states we have $-H(A|B) = \log d_A$, whereas for all separable (i.e., nonentangled) states we have $H(A|B) \geq 0$.

Example 23. Let us explore in more detail how the bound (165) behaves for some illustrative cases.

(1) For maximally entangled states we get

$$q_{\mathrm{MU}} + H(A|B) = q_{\mathrm{MU}} - \log d_A \leq 0, \tag{167}$$

and hence the bound becomes trivial. This is as expected from the guessing game example discussed in Sec. IV.D.1.

(2) For the case when Bob has no memory (i.e., B is trivial), Eq. (165) reduces to (47),

$$H(X) + H(Z) \geq q_{\mathrm{MU}} + H(\rho_A). \tag{168}$$

This is the strengthened Maassen-Uffink relation for mixed states.

(3) If B is not entangled with A (i.e., the state is separable), then $H(A|B) \geq 0$. Hence, we obtain

$$H(X|B) + H(Z|B) \geq q_{\mathrm{MU}}. \tag{169}$$

This last example illustrates that Eq. (165) has applications for entanglement witnessing. More precisely, note that by the data-processing inequality (153), Eq. (165) also implies

$$H(X|Y_B) + H(Z|W_B) \geq q_{\mathrm{MU}} + H(A|B), \tag{170}$$

with $\mathbb{Y}_B$ and $\mathbb{W}_B$ measurements on B. Now violating the q_{MU} lower bound in Eq. (169) implies that the state ρ_{AB} must have been entangled. We discuss this in detail in Sec. VI.D.

Using the following extension of the notation from Sec. III.F to quantum memory:

$$\rho_{K\Theta B} := \frac{1}{2}\sum_k \sum_{j=X,Z} |k\rangle\langle k|_K \otimes |j\rangle\langle j|_\Theta \otimes (\langle k|U_j^\dagger \otimes 1_B)\rho_{AB}(U_j|k\rangle \otimes 1_B), \tag{171}$$

we can rewrite Eq. (165) as

$$H(K|B\Theta) \geq \tfrac{1}{2}[q_{\mathrm{MU}} + H(A|B)]. \tag{172}$$

This is the extension of Eq. (64) to quantum memory. Writing the relation in this way also makes a connection to the guessing game discussed in Sec. IV.D.1; see Fig. 8. We point to Sec. IV.D.7 for a partial extension of Eq. (172) in terms of the more operational min-entropy.

Let us take a step back and look at the history that led up to the uncertainty relation (165). Arguably the first work on uncertainty relations with quantum memory was by Christandl and Winter (2005). Their formulation was restricted to bases that are related by the Fourier matrix but their work captures similar intuition as Eq. (165). The main difference, however, is that their relations are formulated for quantum channels rather than for quantum states. We discuss quantum channel uncertainty relations in Sec. IV.G.

Renes and Boileau (2009) gave the first quantum memory uncertainty relation in terms of the quantum state perspective. However, instead of bipartite states ρ_{AB}, they considered tripartite states ρ_{ABC}.[17] We discuss entropic uncertainty relations for tripartite states in Sec. IV.E. Moreover, there is a close connection between tripartite and bipartite uncertainty relations. In fact, as discussed in Sec. IV.E, Renes and Boileau (2009) conjectured a tripartite uncertainty relation that is equivalent to Eq. (165). Section IV.E also discusses the proof of quantum memory uncertainty relations such as Eq. (165) and notes that the tripartite formulation of (165) naturally generalizes to the Rényi entropy family.

3. Arbitrary measurements

Here we discuss some generalizations of Eq. (165) for arbitrary measurements. Recall from Sec. III.D that the Maassen-Uffink relation generalizes to POVMs with the overlap c given by Eq. (49). In contrast, Eq. (165) holds with c as in (49) if one of the POVMs has rank-one elements (Coles *et al.*, 2011), but it does not hold for general POVMs. This can be remedied in two ways. The approach by Frank and Lieb (2013a) leads to a relation of the form (165) using a weaker complementarity factor. We have

$$H(X|B) + H(Z|B) \geq \log\frac{1}{c''} + H(A|B), \tag{173}$$

where

$$c'' = \max_{x,z} \operatorname{tr}[\mathbb{X}^x\mathbb{Z}^z]. \tag{174}$$

Note that $c'' \geq c$ in general and that c'' reduces to c for measurements in bases. However, one may argue that the form (173) and (174) is not the most natural one if we consider general projective measurements or POVMs. This is best explained by means of an example (Furrer *et al.*, 2014).

Example 24. Consider a quantum system A comprised of two qubits A_1 and A_2, where A_1 is maximally entangled with a second qubit B, and A_2 is in a fully mixed state in product with A_1 and B. We employ rank-two projective measurements $\mathbb{X}_{A_1}$ and $\mathbb{Z}_{A_1}$ which measure A_1 in two MUBs and leave A_2 intact. Analogously, we employ $\mathbb{X}_{A_2}$ and $\mathbb{Z}_{A_2}$ which measure A_2 in two MUBs and leave A_1 intact. Evaluating the terms of interest for the measurement pairs $\{\mathbb{X}_{A_1}, \mathbb{Z}_{A_1}\}$ and $\{\mathbb{X}_{A_2}, \mathbb{Z}_{A_2}\}$ yields $c = 1/2$ and $c'' = 1$ in both cases. Moreover, we find that

$$H(A|B) = H(A_1|B) + H(A_2) = -1 + 1 = 0. \tag{175}$$

Hence, the right-hand side of the Frank and Lieb relation (173) vanishes for both measurement pairs. Indeed, if the maximally entangled system A_1 is measured, we find that

[17] More precisely, Renes and Boileau (2009) established a bipartite uncertainty relation—a special case of Eq. (165) where the $\mathbb{X}$ and $\mathbb{Z}$ bases are related by the Fourier matrix. But they focused their discussion primarily on the tripartite formulation.

$$H(X|B) + H(Y|B) = 0, \tag{176}$$

and the bound in Eq. (173) becomes an equality for the measurement pair $\{\mathbb{X}_{A_1}, \mathbb{Z}_{A_1}\}$. On the other hand, if A_2 is measured instead, we find that

$$H(X|B) + H(Y|B) = 2, \tag{177}$$

and the bound is far from tight for the measurement pair $\{\mathbb{X}_{A_2}, \mathbb{Z}_{A_2}\}$.

Examining this example, it is clear that the expected uncertainty strongly depends on which of the two systems is measured. More generally, it depends on how much entanglement is consumed in the measurement process. However, this information is not taken into account by the overlaps c or c'', nor by the entanglement of the initial state as measured by $H(A|B)$. Example 24 suggests that Eq. (165) can be generalized by considering the difference in entanglement of the state before and after measurement. In fact, Tomamichel (2012) showed the bipartite uncertainty relation

$$H(X|B) + H(Z|B) \geq \log\frac{1}{c'} + H(A|B) - \min\{H(A'|XB), H(A'|ZB)\}, \tag{178}$$

with c' given by Eq. (51). The entropy $H(A'|XB)$ is evaluated for the postmeasurement state

$$\rho_{XA'B} = \sum_x |x\rangle\langle x|_X \otimes (\mathbb{X}_A^x \otimes \mathbb{1}_B)\rho_{AB}(\mathbb{X}_A^x \otimes \mathbb{1}_B), \tag{179}$$

and similarly for $H(A'|ZB)$. (We use $A' = A$ to denote the system A after measurement to avoid confusion.) Notably the term $H(A'|XB)$ vanishes for a measurement given by a basis since in this case the state of A' is pure conditioned on X.

Example 24 (continued). It is straightforward to see that if A_1 (A_2) is measured, the average entanglement left in the postmeasurement state measured by the von Neumann entropy is given by $H(A_2|B)$ [$H(A_1|B)$]. Hence, Eq. (178) turns into

$$H(X|B) + H(Y|B) \geq \log\frac{1}{c} + [H(A|B) - H(A'|B)], \tag{180}$$

where A' corresponds to A_2 (A_1). This inequality is tight for both measurements.

4. Multiple measurements

The basic goal here is to lift some of the relations in Sec. III.G to quantum memory. A general approach for deriving such relations has been provided by Dupuis, Fawzi, and Wehner (2015). As in the unconditional case (cf. Sec. III.G.1), relations for two measurements already imply bounds for larger sets of measurements. For example, supposing A is a qubit and considering the Pauli measurements on A, we find by the simple iterative application of the bound (165) for the measurement pairs $\{\sigma_{\mathbb{X}}, \sigma_{\mathbb{Y}}\}$, $\{\sigma_{\mathbb{X}}, \sigma_{\mathbb{Z}}\}$, and $\{\sigma_{\mathbb{Y}}, \sigma_{\mathbb{Z}}\}$ that

$$H(K|B\Theta) \geq \tfrac{1}{2} + \tfrac{1}{2}H(A|B), \tag{181}$$

with $\Theta \in \{\sigma_{\mathbb{X}}, \sigma_{\mathbb{Y}}, \sigma_{\mathbb{Z}}\}$. Here we use the following extension of the notation from Sec. III.G to quantum memory:

$$\rho_{K\Theta B} := \frac{1}{3}\sum_{k=1,2}\sum_{j=X,Y,Z} |k\rangle\langle k|_K \otimes |j\rangle\langle j|_\Theta \otimes (\langle k|U_j^\dagger \otimes 1_B)\rho_{AB}(U_j|k\rangle \otimes 1_B). \tag{182}$$

Note that alternatively the left-hand side of Eq. (181) might also be written as

$$H(K|B\Theta) = \tfrac{1}{3}[H(K|B\Theta = \sigma_{\mathbb{X}}) + H(K|B\Theta = \sigma_{\mathbb{Y}}) + H(K|B\Theta = \sigma_{\mathbb{Z}})], \tag{183}$$

where

$$\rho_{KB|\Theta=\sigma_{\mathbb{X}}} := \sum_{k=1,2} |k\rangle\langle k|_K \otimes (\langle k|U_X^\dagger \otimes 1_B)\rho_{AB}(U_X|k\rangle \otimes 1_B), \tag{184}$$

and similarly for $\sigma_{\mathbb{Y}}$, $\sigma_{\mathbb{Z}}$. The goal in the following sections is to find uncertainty relations that are stronger than any bounds that can be directly derived from relations for two measurements.

5. Complex projective two-designs

Berta, Coles, and Wehner (2014) showed that the uncertainty equality (82) in terms of the collision entropy for a full set of MUBs also holds with quantum memory. That is, for any bipartite state ρ_{AB} with a full set of $d+1$ MUBs on the d-dimensional A system,

$$H_{\text{coll}}(K|B\Theta) = \log(d+1) - \log\left(2^{-H_{\text{coll}}(A|B)} + 1\right), \tag{185}$$

with $\Theta \in \{\theta_1, \ldots, \theta_{d+1}\}$, Here, as in Eq. (171), we use the notation

$$\rho_{K\Theta B} := \frac{1}{d+1}\sum_{k=1}^{d}\sum_{j=1}^{d+1} |k\rangle\langle k|_K \otimes |j\rangle\langle j|_\Theta \otimes (\langle k|U_j^\dagger \otimes 1_B)\rho_{AB}(U_j|k\rangle \otimes 1_B). \tag{186}$$

Example 25. For the qubit Pauli measurements Eq. (185) yields

$$H_{\text{coll}}(K|B\Theta) = \log 3 - \log\left(2^{-H_{\text{coll}}(A|B)} + 1\right) \quad \text{with} \quad \Theta \in \{\sigma_{\mathbb{X}}, \sigma_{\mathbb{Y}}, \sigma_{\mathbb{Z}}\}. \tag{187}$$

Since the collision entropy has an interpretation in terms of the pretty good guessing probability (139),

$$H_{\text{coll}}(X|B) = -\log p_{\text{guess}}^{\text{pg}}(X|B), \tag{188}$$

and the pretty good recovery map (148),

$$H_{\mathrm{coll}}(A|B) = -\log[d_A \cdot F^{\mathrm{pg}}(A|B)], \tag{189}$$

the uncertainty equality (185) can be understood as an entanglement-assisted game of guessing complementary measurement outcomes (as described in Sec. IV.D.1). Namely, we can rewrite Eq. (185) as

$$p^{\mathrm{pg}}_{\mathrm{guess}}(K|B\Theta) = \frac{d \cdot F^{\mathrm{pg}}(A|B) + 1}{d+1}. \tag{190}$$

This gives a one-to-one relation between uncertainty (certainty) as measured by $p^{\mathrm{pg}}_{\mathrm{guess}}(K|B\Theta)$ and the absence (presence) of entanglement as measured by $F^{\mathrm{pg}}(A|B)$. In contrast, quantum memory assisted uncertainty relations for two measurements, e.g., as in Eq. (172), provide us only with a connection between uncertainty and entanglement in one direction. Namely, they state that low uncertainty implies the presence of entanglement (cf. Sec. VI.D).

The uncertainty equality (185) is derived by extending the proof from Ballester and Wehner (2007) who made use of the fact that a full set of mutually unbiased bases generates a complex projective two-design (Klappenecker and Rotteler, 2005). From this, it is also immediately apparent that an equality such as Eq. (185) holds for other complex projective two-designs as well. This includes, in particular, so-called symmetric informationally complete positive operator-valued measures: SIC-POVMs.[18] More precisely, any SIC-POVM

$$\left\{\frac{1}{d}|\psi_k\rangle\langle\psi_k|\right\}_{k=1}^{d^2} \tag{191}$$

gives rise to the uncertainty equality

$$H_{\mathrm{coll}}(K|B\Theta) = \log[d(d+1)] - \log\left(2^{-H_{\mathrm{coll}}(A|B)} + 1\right), \tag{192}$$

with $\Theta \in \{\theta_1, \ldots, \theta_{d+1}\}$. Other examples that generate complex projective two designs are unitary two-designs.[19] This includes, in particular, the Clifford group for n qubit systems.

Berta, Fawzi, and Wehner (2014) also showed that Eq. (185) for a full set of $d+1$ MUBs generates the following relation in terms of the von Neumann entropy:

$$H(K|B\Theta) \geq \log(d+1) - 1 + \min\{0, H(A|B)\}, \tag{193}$$

with $\Theta \in \{\theta_1, \ldots, \theta_{d+1}\}$. This corresponds to the generalization of Eq. (81) to quantum memory. Note that the entropy dependent term on the right-hand side makes a contribution only if the conditional entropy $H(A|B)$ is negative. This is consistent with Eq. (81).

For smaller sets of $L < d+1$ MUBs, Berta, Coles, and Wehner (2014) extended Eq. (91) to quantum memory,

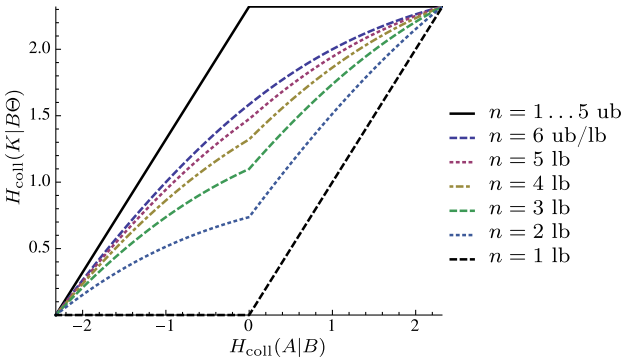


FIG. 9. For $d = 5$ and a various number of MUBs $n \leq d+1 = 6$ the lower bounds (lb) are plotted on the entropic uncertainty $H_{\mathrm{coll}}(K|\Theta)$ from Eq. (194) as a function of $H_{\mathrm{coll}}(A|B)$. Moreover, for $n < 6$ we have only the trivial upper bound (ub) on $H_{\mathrm{coll}}(K|B\Theta)$, whereas for $n = 6$ the lower and upper bounds coincide as in Eq. (185).

$$H_{\mathrm{coll}}(K|B\Theta) \geq \begin{cases} -\log\frac{d\cdot 2^{-H_{\mathrm{coll}}(A|B)}+L-1}{L\cdot d} & \text{for } H_{\mathrm{coll}}(A|B) \geq 0, \\ -\log\frac{d+(L-1)2^{-H_{\mathrm{coll}}(A|B)}}{L\cdot d} & \text{for } H_{\mathrm{coll}}(A|B) < 0, \end{cases} \tag{194}$$

with $\Theta \in \{\theta_1, \ldots, \theta_L\}$. Moreover, for all d and L there exist states that achieve equality. Note that for $L = d+1$ the distinction of cases in Eq. (194) collapses and furthermore becomes an upper bound as shown in Eq. (185). In Fig. 9 we illustrate this by means of an example for $d = 5$ (with $L \leq 6$).

6. Measurements in random bases

In the unconditional case we found that measurements in random bases lead to strong uncertainty relations as, e.g., in Eq. (98). Hence, we might expect that we can generalize this to quantum memory,

$$H(K|B\Theta) \overset{?}{\geq} O\left(\log d \cdot \left(1 - \frac{1}{L}\right)\right) + \min\{0, H(A|B)\}, \tag{195}$$

with $\Theta \in \{\theta_1, \ldots, \theta_L\}$ chosen at random. Unfortunately, the previous works (Fawzi, Hayden, and Sen, 2011; Adamczak *et al.*, 2016) make use of measure concentration and ε-nets arguments that seem to fail for quantum memory. It is, however, possible to use some of the techniques from Berta, Coles, and Wehner (2014) based on operator Chernoff bounds to derive relations of the form (195). The downside is that we get only strong uncertainty relations for a large number L of measurements,

$$L \geq O(d\log(d)). \tag{196}$$

We conclude that it is an open problem to show the existence of small(er) sets of $L > 2$ measurements that generate strong uncertainty relations that hold with quantum memory.

[18] See Renes *et al.* (2004) for a detailed discussion of SIC-POVMs.

[19] See Dankert *et al.* (2009) for a detailed discussion of unitary two-designs.

7. Product measurements on multiple qubits

Let us now consider uncertainty relations for multiple-qubit systems, which have applications in quantum cryptography. For historical reasons we start with the n qubit six-state measurements and discuss only the BB84 measurements afterward (see Sec. III.G.5 for definitions of these measurements). For the six-state measurements, Berta (2013) showed that for any bipartite state ρ_{A^nB} with the A^n system given by n qubits,

$$H_{\mathrm{coll}}(K^n|B\Theta^n) \geq n \cdot \log\tfrac{3}{2} + 1 - \log\left(2^{-H_{\mathrm{coll}}(A^n|B)} + 1\right), \tag{197}$$

with $\Theta^n \in \{\theta_1, \ldots, \theta_{3^n}\}$. This extends Eq. (187) from 1 to n qubits. The bound (197) also implies a similar relation in terms of the von Neumann entropy (Berta, Fawzi, and Wehner, 2014), extending Eq. (105) to

$$H(K^n|B\Theta^n) \geq n \cdot \log\tfrac{3}{2} + \min\{0, H(A^n|B)_\rho\}, \tag{198}$$

with $\Theta^n \in \{\theta_1, \ldots, \theta_{3^n}\}$. Moreover, Dupuis, Fawzi, and Wehner (2015) improved Eq. (197) to the conceptually different bound

$$H_{\mathrm{coll}}(K^n|B\Theta^n) \geq n \cdot \gamma_{6s}\left(\frac{H_{\mathrm{coll}}(A^n|B)}{n}\right) - 1, \tag{199}$$

where

$$\gamma_{6s}(x) := \begin{cases} x & \text{if } x \geq \log 3/2, \\ f^{-1}(x)\log 3 & \text{if } 0 < x < \log 3/2, \end{cases} \tag{200}$$

with $f(x) = h_{\mathrm{bin}}(x) + x\log 3 - 1$ and h_{bin} denotes the binary entropy. Using the equivalence between the collision entropy and the min-entropy from Eq. (142) this readily implies a relation as Eq. (199), but with both the collision entropy terms H_{coll} replaced with min-entropy terms $H_{\min}$. Importantly, this variant remains nontrivial for all values of $H_{\min}(A^n|B)$. Also, Dupuis, Fawzi, and Wehner (2015) established a meta theorem that can be used to derive uncertainty relations also for other kinds of measurements.

For the n qubit BB84 measurements Dupuis, Fawzi, and Wehner (2015) found

$$H_{\mathrm{coll}}(K^n|B\Theta^n) \geq n \cdot \gamma_{BB84}\left(\frac{H_{\mathrm{coll}}(A^n|B)}{n}\right) - 1, \tag{201}$$

with $\Theta^n \in \{\theta_1, \ldots, \theta_{2^n}\}$, where

$$\gamma_{BB84}(x) := \begin{cases} x & \text{if } x \geq \frac{1}{2}, \\ g^{-1}(x) & \text{if } 0 < x < \frac{1}{2}, \end{cases} \tag{202}$$

with $g(x) = h_{\mathrm{bin}}(x) + x - 1$. Again using the equivalence between the collision entropy and the min-entropy from Eq. (142), we get a relation as Eq. (201) but with both the collision entropy terms H_{coll} replaced with min-entropy terms $H_{\min}$. We note that this is also nontrivial for one qubit ($n = 1$) and only the two measurements $\Theta \in \{\sigma_{\mathbb{X}}, \sigma_{\mathbb{Z}}\}$. Equation (201) and its min-entropy analog can be understood in terms of the bipartite guessing game with quantum memory as mentioned in Sec. IV.D.1.

8. General sets of measurements

Section III.G.6 discussed the work of Liu, Mu, and Fan (2015) for unipartite systems without memory. Here we note that they also gave bipartite uncertainty relations with quantum memory. Again for simplicity we state the case only of $L = 3$ observables (in any dimension $d \geq 2$). We find as the direct extension of Eq. (106),

$$H(K|B\Theta) \geq \frac{1}{3}\log\frac{1}{m} + \frac{2}{3}H(A|B), \tag{203}$$

with $\Theta \in \{V^{(1)}, V^{(2)}, V^{(3)}\}$, where the multiple overlap constant m is defined as in Eq. (107). As in the unconditional case, this has to be compared with the bounds implied by two measurement relations as in Eq. (181). See Liu, Mu, and Fan (2015) for a fully worked out example where Eq. (203) can become stronger than any bounds implied by two measurement relations.

E. Tripartite quantum memory uncertainty relations

1. Tripartite uncertainty relation

The physical scenario corresponding to tripartite uncertainty relations is shown in Fig. 10. Suppose there is a source that outputs the systems ABC in state ρ_{ABC}. Systems A, B, and C are, respectively, sent to Alice, Bob, and Charlie. Then Alice performs either the $\mathbb{X}$ or $\mathbb{Z}$ measurement. If she

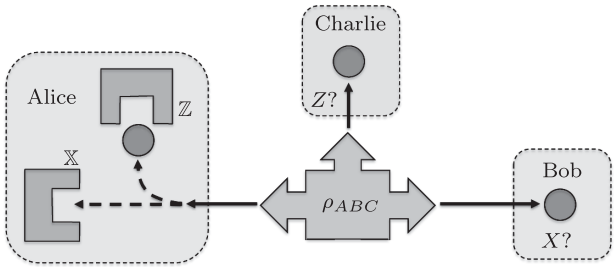


FIG. 10. Diagram of the tripartite quantum memory setup. First, a source prepares ABC in state ρ_{ABC}, and sends A to Alice, B to Bob, and C to Charlie. Second, Alice measures either $\mathbb{X}$ or $\mathbb{Z}$ on A and asks how uncertain is Bob about her X outcome, given B, and how uncertain is Charlie about her Z outcome, given C? As shown in Eq. (206) there is a trade-off that is quantified by the complementarity of the measurements X and Z. W interpret this scenario as a guessing game, also called a monogamy game. In this game, Bob and Charlie play against Alice. They prepare ρ_{ABC} where they send A to Alice, Bob keeps B, and Charlie keeps C. Alice then randomly chooses a measurement obtaining the measurement outcome K. Afterward, she sends her choice of basis to Bob and Charlie. They win the game if and only if both output K. This game measures the same kind of uncertainty as Eq. (206), explicitly exploiting the monogamy of entanglement: if Bob produces $K = X$ correctly in case Alice measured $\mathbb{X}$, then this is a certificate that Charlie cannot produce a good guess of $K = Z$ in case Alice measured $\mathbb{Z}$.

measures $\mathbb{X}$, then Bob's goal is to minimize his uncertainty about X. If she measures $\mathbb{Z}$, then Charlie's goal is to minimize his uncertainty about Z. Renes and Boileau (2009) considered exactly this scenario but restricted to the case where the $\mathbb{X}$ and $\mathbb{Z}$ bases are related by the Fourier matrix F,

$$|\mathbb{X}^x\rangle = F|\mathbb{Z}^x\rangle \quad \text{with} \quad F = \sum_{z,z'} \frac{\omega^{-zz'}}{\sqrt{d}} |\mathbb{Z}^z\rangle\langle\mathbb{Z}^{z'}|, \tag{204}$$

where $\omega = e^{2\pi i/d}$. Notice that this makes $\mathbb{X}$ and $\mathbb{Z}$ mutually unbiased, although in general not all pairs of MUBs are related by the Fourier matrix. They quantified Bob's and Charlie's uncertainties in terms of the conditional entropies $H(X|B)$ and $H(Z|C)$, respectively, and proved that any tripartite state ρ_{ABC} satisfies

$$H(X|B) + H(Z|C) \geq \log d. \tag{205}$$

Here d is the dimension of the A system and the classical-quantum states ρ_{XB} and ρ_{ZC} are defined similarly as in Eq. (166). Renes and Boileau (2009) also conjectured that this relation generalizes to arbitrary measurements given by bases,

$$H(X|B) + H(Z|C) \geq q_{\mathrm{MU}}, \tag{206}$$

with q_{MU} as in Eq. (31). Intuitively, what Eq. (205) says is that the more Bob knows about Z, the less Charlie knows about X, and vice versa. This is a signature of the well-known trade-off *monogamy of entanglement*, which roughly says that the more Bob is entangled with Alice, the less he is with Charlie.[20] The trade-off described by Eqs. (205) and (206) can be viewed as a fine-grained notion of this monogamy. Namely, the monogamy appears at the level of measurement pairs $(\mathbb{X}, \mathbb{Z})$.

Also note that Eq. (206) implies both the Maassen-Uffink relation (31) and its classical memory extension (164), due to the data-processing inequality (153). That is,

$$H(X|B) \leq H(X|Y) \leq H(X), \tag{207}$$

for any measurement $\mathbb{Y}$ on B. As seen in Sec. IV.E.3 the quantum memory extension (206) is strictly stronger than the classical memory extension (164).

2. Proof of quantum memory uncertainty relations

The quantum memory uncertainty relation (206) was first proved by Berta *et al.* (2010). Although they explicitly stated their relation in the bipartite form (165), they noted that two relations are equivalent.

The equivalence between the bipartite and tripartite relations can be seen as follows. To obtain the bipartite relation (165) from the tripartite relation (206), apply the latter to a purification $|\psi\rangle_{ABC}$ of ρ_{AB}. Now for tripartite pure states we have

$$H(Z|C) = H(Z|B) - H(A|B), \tag{208}$$

and inserting this into Eq. (206) gives Eq. (165). Conversely we first prove Eq. (206) for tripartite pure states $|\psi\rangle_{ABC}$ by inserting Eq. (208) into Eq. (165). Then note that the proof for mixed states ρ_{ABC} follows by applying Eq. (206) to a purification $|\psi\rangle_{ABCD}$ of ρ_{ABC}, and making use of the data-processing inequality (153),

$$H(Z|CD) \leq H(Z|C). \tag{209}$$

The original proof of Eq. (206) was based on so-called smooth entropies.[21] The proof was subsequently simplified by Coles *et al.* (2011) and Tomamichel and Renner (2011), which culminated in the concise proof given by Coles *et al.* (2012). The latter proof distills the main ideas of the previous proofs: the use of duality relations for entropies as in Eq. (154) and the data-processing inequality as in Eq. (153). More generally, the proof technique applies to a whole family of entropies satisfying a few axioms (including the Rényi entropies). We present the proof in Appendix C.3. Finally, we note that a direct matrix analysis proof was given by Frank and Lieb (2013a).

3. Quantum memory tightens the bound

Here we argue that the tripartite uncertainty relation in terms of quantum memory (206) is tighter than the corresponding relation in terms of classical memory (164). We explain that there exist states ρ_{ABC} for which Eq. (206) is an equality but Eq. (164) is loose, even if one optimizes over all choices of measurements on B and C.

Let us introduce some notation. Consider a bipartite state ρ_{AB} and let $\mathbb{X}_A$ and $\mathbb{Y}_B$ be measurements on systems A and B, respectively. Now, how small can we make the uncertainty $\mathbb{X}_A$ given that we can optimize over all choices of $\mathbb{Y}_B$? That is, consider the quantity

$$\alpha(\mathbb{X}_A, \rho_{AB}) \coloneqq \min_{\mathbb{Y}_B} H(X_A|Y_B). \tag{210}$$

This is to be compared to the classical-quantum conditional entropy

$$\beta(\mathbb{X}_A, \rho_{AB}) \coloneqq H(X_A|B). \tag{211}$$

Because of the data-processing inequality (153), we have that

$$\alpha(\mathbb{X}_A, \rho_{AB}) \geq \beta(\mathbb{X}_A, \rho_{AB}), \tag{212}$$

and naively one might guess that Eq. (212) is satisfied with equality in general. However, this is false (Hiai and Petz, 1991; DiVincenzo *et al.*, 2004). In general there is a nonzero gap $\alpha - \beta > 0$. There are many examples to illustrate this; in fact one can argue that most states ρ_{AB} exhibit a gap between α and β (Dupuis *et al.*, 2013). This phenomenon is called locking, discussed in Sec. VI.H.3. It is closely related to a measure of quantum correlations known as quantum discord

[20] See Horodecki *et al.* (2009) for an in-depth review about entanglement.

[21] See Tomamichel (2016) for an introduction to smooth entropies.

(Ollivier and Zurek, 2001; Modi *et al.*, 2012). Nonzero discord is associated with the potential to have a gap between α and β. We discuss discord in more detail in Sec. VI.H.2. For now note that discord is defined as

$$D(A|B) \coloneqq \min_{\mathbb{Y}_B} H(A|Y_B) - H(A|B), \tag{213}$$

where the optimization is over all POVMs $\mathbb{Y}_B$ on B.

Example 26. Let $\mathbb{X}_A = \{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ and consider the bipartite quantum state

$$\rho_{AB} = \tfrac{1}{2}(|0\rangle\langle 0| \otimes |0\rangle\langle 0| + |1\rangle\langle 1| \otimes |+\rangle\langle +|). \tag{214}$$

For this state, the gap between α and β is precisely given by the discord

$$D(A|B) = \alpha(\mathbb{X}_A, \rho_{AB}) - \beta(\mathbb{X}_A, \rho_{AB}). \tag{215}$$

It is known that $D(A|B) = 0$ if and only if system B is classical, i.e., if ρ_{AB} is a quantum-classical state. But the state ρ_{AB} in Eq. (214) is not quantum classical. Hence, $D(A|B) > 0$ and we have $\alpha > \beta$.

Now we give an example state for which the quantum memory relation (206) is an equality but the measured relation (164) is loose.

Example 27. Consider the tripartite pure state $|\psi\rangle_{ABC} = (|000\rangle + |11+\rangle)/\sqrt{2}$, with $\mathbb{Z}$ being the standard basis and $\mathbb{X}$ being the $\{|+\rangle, |-\rangle\}$ basis. We have

$$H(Z|C) = 1 - H(\rho_C) \approx 0.4, \tag{216}$$

$$H(X|B) = H(\rho_C) \approx 0.6. \tag{217}$$

Hence, this state satisfies the quantum memory relation (205) with equality,

$$H(X|B) + H(Z|C) = 1. \tag{218}$$

However, the classical memory relation (164) is not satisfied with equality. This follows from example 26, noting that ρ_{AC} is the same state as in Eq. (214).

4. Tripartite guessing game

Tripartite uncertainty relations can be understood in the language of guessing games as outlined in Fig. 10. Tomamichel *et al.* (2013) showed that there is a fundamental trade-off between Bob's guessing probability $p_{\text{guess}}(K|B\Theta)$ and Charlie's guessing probability $p_{\text{guess}}(K|C\Theta)$,

$$p_{\text{guess}}(K|B\Theta) + p_{\text{guess}}(K|C\Theta) \leq 2b, \tag{219}$$

with the overlap b as in Eq. (40). Alternatively, one can rewrite this in terms of the min-entropy using the concavity of the logarithm,

$$H_{\min}(K|B\Theta) + H_{\min}(K|C\Theta) \geq 2\log\frac{1}{b}. \tag{220}$$

Note that Eq. (220) is an extension of Eq. (71) to the tripartite scenario. This relation again shows a trade-off between Bob's and Charlie's winning probabilities, which are closely connected to the idea of monogamy of entanglement (cf. Sec. IV.E.1).

5. Extension to Rényi entropies

The Maassen-Uffink relation for Rényi entropies (35) naturally generalizes to a tripartite uncertainty relation with quantum memory. It is expressed in terms of the conditional Rényi entropies, whose definition and properties are discussed in Appendix C. For these entropies, the following relation holds (Coles *et al.*, 2012)[22]:

$$H_\alpha(X|B) + H_\beta(Z|C) \geq q_{\text{MU}} \quad \text{for } \frac{1}{\alpha} + \frac{1}{\beta} = 2. \tag{221}$$

Notably, the tripartite uncertainty relation (206) is the special case where $\alpha = \beta = 1$. Another interesting special case is $\alpha = \infty$ and $\beta = 1/2$, which, respectively, correspond to the min- and max-entropies introduced in Eqs. (138) and (155). The resulting relation,

$$H_{\min}(X|B) + H_{\max}(Z|C) \geq q_{\text{MU}}, \tag{222}$$

was first proved by Tomamichel and Renner (2011) and is fundamental to quantum key distribution (see Sec. VI.B).

6. Arbitrary measurements

All of the tripartite uncertainty relations can be generalized to arbitrary POVMs $\mathbb{X}$ and $\mathbb{Z}$. Coles *et al.* (2011) and Tomamichel and Renner (2011) independently noted that Eq. (206) holds for POVMs with the overlap c given by Eq. (49). This was strengthened by Tomamichel (2012) to the overlap c' given by Eq. (51). Further strengthening was given by Coles and Piani (2014b). However, their bound is implicit, involving an optimization of a single real-valued parameter over a bounded interval. Namely, they showed a lower bound

$$q_{\text{CP2}} \coloneqq \max_{0\leq p\leq 1} \lambda_{\min}(\Delta(p)), \tag{223}$$

where $\lambda_{\min}[\cdot]$ denotes the minimum eigenvalue and

$$\Delta(p) \coloneqq p\delta(\mathbb{X}, \mathbb{Z}) + (1-p)\delta(\mathbb{Z}, \mathbb{X}), \tag{224}$$

$$\delta(\mathbb{X}, \mathbb{Z}) \coloneqq \sum_x a_x(\mathbb{X}, \mathbb{Z}) \cdot \mathbb{X}^x, \tag{225}$$

$$a_x(\mathbb{X}, \mathbb{Z}) \coloneqq -\log\left\| \sum_z \mathbb{Z}^z \mathbb{X}^x \mathbb{Z}^z \right\|. \tag{226}$$

[22]The relation follows from the work (Coles *et al.*, 2012) in conjunction with properties of the conditional Rényi entropy presented by Müller-Lennert *et al.* (2013). It is thus first mentioned in the later work (Müller-Lennert *et al.*, 2013). Notably, Coles *et al.* (2012) proved a tripartite uncertainty relation for a different definition of the conditional Rényi entropy (Tomamichel, Colbeck, and Renner, 2009).

Using the fact that $\delta(\mathbb{X},\mathbb{Z}) \geq \min_x a_x(\mathbb{X},\mathbb{Z})\cdot\mathbb{1}$, it is straightforward to show that $q_{\mathrm{CP2}} \geq \log(1/c')$.

F. Mutual information approach

While entropy quantifies the lack of information, it is both intuitive and useful to also consider measures that quantify the presence of information or correlation. Consider the mutual information $I(X:Y)$, which quantifies the correlation between random variables X and Y and is given by

$$I(X:Y) \coloneqq H(X) + H(Y) - H(XY) \tag{227}$$

$$= H(X) - H(X|Y). \tag{228}$$

It quantifies the information gained—or equivalently, the reduction of ignorance—about X when given access to Y. It is worth noting that the mutual information is particularly well suited for applications in information theory. For example, the capacity of a channel can be expressed in terms of its mutual information (Shannon, 1948), that is, in terms of the correlations between a receiver and a sender. Hence, we also discuss the application of "information exclusion relations" (uncertainty relations expressed via the mutual information) to information transmission over channels.

1. Information exclusion principle

Hall (1995, 1997) pioneered an alternative formulation of the uncertainty principle based on the mutual information, which he called the *information exclusion principle*. Information exclusion relations are closely related to entropic uncertainty relations that allow for memory. The idea is that one is interested in the trade-off between a memory system Y being correlated to $\mathbb{X}$ versus being correlated to $\mathbb{Z}$ (with $\mathbb{X}$ and $\mathbb{Z}$ being two measurements on some quantum system A).

2. Classical memory

We show now how information exclusion relations follow directly from entropic uncertainty relations (Hall, 1995). Consider a generic uncertainty relation involving Shannon entropy terms of the form $\sum_{n=1}^{N} H(X_n)_\rho \geq q$ as in Eq. (157). Recall the discussion in Sec. IV.C which showed that the uncertainty relation $\sum_{n=1}^{N} H(X_n|Y) \geq q$ as in Eq. (160) immediately follows, where Y is some classical memory. Now with the definition of the mutual information (227) we can rewrite this as

$$\sum_{n=1}^{N} H(X_n) - I(X_n:Y) \geq q. \tag{229}$$

We have $H(X_n) \leq \log d$ for each n with d the dimension of the quantum system A that is measured. Combining this with Eq. (229) gives

$$\sum_{n=1}^{N} I(X_n:Y) \leq N\log d - q. \tag{230}$$

For example, if we take the Maassen-Uffink relation (31) as the starting point, we end up with

$$I(X:Y) + I(Z:Y) \leq \log(d^2 c) =: r_{\mathrm{H}}. \tag{231}$$

The information exclusion relation in Eq. (231) was presented by Hall (1995). Note that we have $\log d \leq r_{\mathrm{H}} \leq 2\log d$, with r_{H} reaching the extreme points, respectively, for $c = 1/d$ and $c = 1$. Equation (231) has an intuitive interpretation: any classical memory cannot be highly correlated to two complementary measurement outcomes of a quantum system. In the fully complementary case, the bound becomes $r_{\mathrm{H}} = \log d$, implying that if the classical memory is perfectly correlated to X, $I(X:Y) = \log d$, then it must be completely uncorrelated to Z, $I(Z:Y) = 0$.

3. Stronger bounds

Note that Eq. (231) uses the same overlap c as appearing in the Maassen-Uffink uncertainty relation (31). However, Grudka *et al.* (2013) realized that this often leads to a fairly weak bound. They noted that the complementarity of the mutual information should depend not only on the maximum element c of overlap matrix $[c_{xz}]$ [see Eq. (32) for its definition], but also on other elements of this matrix. They conjectured a stronger information exclusion relation of the form $I(X:Y) + I(Z:Y) \leq r_{\mathrm{G}}$ with

$$r_{\mathrm{G}} = \log_2\left(d \cdot \sum_{\text{d largest}} c_{xz}\right), \tag{232}$$

with the sum over the largest d terms of the matrix $[c_{xz}]$. This conjecture was proved by Coles and Piani (2014b), where the bound was further strengthened to

$$I(X:Y) + I(Z:Y) \leq r_{\mathrm{CP}}, \tag{233}$$

with

$$r_{\mathrm{CP}} \coloneqq \min\{r(\mathbb{X},\mathbb{Z}), r(\mathbb{Z},\mathbb{X})\}, \tag{234a}$$

$$r(\mathbb{X},\mathbb{Z}) \coloneqq \log\left(d\sum_x \max_z c_{xz}\right), \tag{234b}$$

$$r(\mathbb{Z},\mathbb{X}) \coloneqq \log\left(d\sum_z \max_x c_{xz}\right). \tag{234c}$$

One can easily verify that $r_{\mathrm{CP}} \leq r_{\mathrm{G}} \leq r_{\mathrm{H}}$.

Example 28. The unitary in Eq. (43) from example 8 provides a simple example where all three bounds are different, namely, $r_{\mathrm{H}} = \log 6$, $r_{\mathrm{G}} = \log 5$, and $r_{\mathrm{CP}} = \log(9/2)$.

Note that the behavior of the bounds r_{H} and r_{CP} are qualitatively different in that they become trivial under different conditions. The former is trivial if at least one row or column of $[c_{xz}]$ is trivial (i.e., composed of all zeros except for one element being 1), whereas the latter is trivial only if all rows and columns $[c_{xz}]$ are trivial. Hence, the latter gives a nontrivial bound for a much larger range of scenarios.

4. Quantum memory

It is natural to ask whether system Y can be generalized to a quantum memory B. Coles and Piani (2014b) showed that Eq. (233) indeed extends to

$$I(X:B) + I(Z:B) \leq r_{\mathrm{CP}} - H(A|B). \tag{235}$$

Here the quantum mutual information of a bipartite quantum state ρ_{AB} is defined as

$$I(A:B) \coloneqq H(\rho_A) + H(\rho_B) - H(\rho_{AB}) \tag{236}$$

$$= H(\rho_A) - H(A|B), \tag{237}$$

and evaluated on the classical-quantum state ρ_{XB} as in Eq. (166). Note that if we specialize to the case where $B = Y$ is classical, then $H(A|Y) \geq 0$ and hence Eq. (235) also implies (233).

Example 29. Consider a maximally entangled state ρ_{AB} for which both $I(X:B)$ and $I(Z:B)$ become equal to $\log d$. Hence, the upper bound r_{CP} must be weakened in such a way that it becomes trivial, and indeed the term $-H(A|B)$ accomplishes this. Namely, we have $-H(A|B) = \log d$ for the maximally entangled state.

In general, a negative value of $H(A|B)$ implies that ρ_{AB} has distillable entanglement (Devetak and Winter, 2005), and this results in a bound in Eq. (235) that is larger than r_{CP}. In the other extreme, when $H(A|B)$ is positive, which intuitively means that the correlations between Alice and Bob are weak, Eq. (235) strengthens the bound in (233).

5. A conjecture

Following the resolved conjectures by Kraus (1987), Renes and Boileau (2009), and Grudka *et al.* (2013), we point to a recent open conjecture by Schneeloch, Broadbent, and Howell (2014). They ask if for any bipartite quantum state ρ_{AB},

$$I(X_A:X_B) + I(Z_A:Z_B) \overset{?}{\leq} I(A:B), \tag{238}$$

where X_A and Z_A are the registers associated with measuring two MUBs $\mathbb{X}_A$ and $\mathbb{Z}_A$ on system A, and likewise for X_B and Z_B on system B. Equation (238) says that the quantum mutual information is lower bounded by the sum of the classical mutual informations in two mutually unbiased bases. We note that a stronger conjecture, in which X_B and Z_B are replaced by the quantum memory B, is violated in general.

G. Quantum channel formulation

1. Bipartite formulation

Christandl and Winter (2005) considered the question of how well information can be transmitted over a quantum channel. A quantum channel is the general form for quantum dynamics (Davies, 1976) (more general than unitary evolution). Mathematically a quantum channel $\mathcal{E}$ is a completely positive trace-preserving map and can be represented in its Kraus form,

$$\mathcal{E}(\cdot) = \sum_j K_j(\cdot)K_j^\dagger, \quad \text{where} \sum_j K_j^\dagger K_j = \mathbb{1}. \tag{239}$$

Christandl and Winter (2005) addressed the topic of sending classical information over a quantum channel, or more specifically, sending two complementary types of classical information over a quantum channel. They considered a scenario where Alice chooses a state, with probability $1/d$, from a set of d orthonormal states, which we label as $\mathbb{Z} = \{|\mathbb{Z}^z\rangle\langle\mathbb{Z}^z|\}$. She then sends the state over the channel $\mathcal{E}$ to Bob, and Bob tries to distinguish which state she sent. Likewise Alice and Bob may play the same game but with the $\mathbb{X} = \{|\mathbb{X}^x\rangle\langle\mathbb{X}^x|\}$ states instead, where the $\mathbb{X}$ and $\mathbb{Z}$ states are related by the Fourier matrix F, given by Eq. (204). Bob's distinguishability for the $\mathbb{Z}$ states can be quantified by the so-called Holevo quantity (Holevo, 1973),

$$\chi(\mathcal{E},\mathbb{Z}) = H\left(\sum_z \frac{1}{d}\mathcal{E}(|\mathbb{Z}^z\rangle\langle\mathbb{Z}^z|)\right) - \sum_z \frac{1}{d} H[\mathcal{E}(|\mathbb{Z}^z\rangle\langle\mathbb{Z}^z|)]. \tag{240}$$

Likewise, $\chi(\mathcal{E},\mathbb{X})$ is a measure of Bob's distinguishability for the $\mathbb{X}$ states. Christandl and Winter (2005) proved that

$$\chi(\mathcal{E},\mathbb{X}) + \chi(\mathcal{E},\mathbb{Z}) \leq \log d + I_{\mathrm{coh}}\left(\frac{\mathbb{1}}{d},\mathcal{E}\right), \tag{241}$$

where the coherent information $I_{\mathrm{coh}}(\rho,\mathcal{E})$ is a measure of the quality of a quantum channel $\mathcal{E}$ introduced by Schumacher and Nielsen (1996). For the maximally mixed input state $\mathbb{1}/d$ it is given by

$$I_{\mathrm{coh}}\left(\frac{\mathbb{1}}{d},\mathcal{E}\right) = H[\mathcal{E}(\mathbb{1}/d)] - H[(\mathcal{I}\otimes\mathcal{E})(|\Phi\rangle\langle\Phi|)], \tag{242}$$

where $|\Phi\rangle = \sum_j (1/\sqrt{d})|j\rangle|j\rangle$ is a maximally entangled state. Coles *et al.* (2011) noted that Eq. (241) holds for arbitrary MUBs, and that it naturally generalizes to arbitrary orthonormal bases $\mathbb{X}$ and $\mathbb{Z}$ with the right-hand side of Eq. (241) replaced by

$$\log(d^2 c) + I_{\mathrm{coh}}\left(\frac{\mathbb{1}}{d},\mathcal{E}\right). \tag{243}$$

Later this bound was improved by Coles and Piani (2014b) to

$$r_{\mathrm{CP}} + I_{\mathrm{coh}}\left(\frac{\mathbb{1}}{d},\mathcal{E}\right). \tag{244}$$

While Eq. (241) may look similar to some uncertainty relations discussed in this section, especially Eq. (235), it is important to note the conceptual difference. The relations discussed previously were from a static perspective, whereas Eq. (240) refers to a dynamic perspective involving a sender and a receiver. Intuitively, what Eq. (241) says is that if Alice can transmit both the $\mathbb{Z}$ states and the $\mathbb{X}$ states well to Bob,

then $\mathcal{E}$ is a noiseless quantum channel, i.e., it is close to a perfect channel (as quantified by the coherent information).

2. Static-dynamic isomorphism

With that said, there is a close, mathematical relationship between the static and dynamic perspectives. In fact, there is an isomorphism, known as the Choi-Jamiołkowski isomorphism (Jamiołkowski, 1972; Choi, 1975) that relates the two perspectives [see, e.g., Życzkowski and Bengtsson (2004)]. Every quantum channel $\mathcal{E}$ corresponds to a bipartite mixed state defined by

$$\rho_{AB} = (\mathcal{I} \otimes \mathcal{E})(|\Phi\rangle\langle\Phi|), \tag{245}$$

where $|\Phi\rangle = \sum_j (1/\sqrt{d})|j\rangle|j\rangle$ is maximally entangled [see Fig. 11(a)]. Note that ρ_{AB} has the property that $\rho_A = \mathrm{tr}_B(\rho_{AB}) = \mathbb{1}/d_A$ is maximally mixed. Likewise, every bipartite mixed state ρ_{AB} with marginal $\rho_A = \mathbb{1}/d_A$ corresponds to a quantum channel whose action on some operator O is defined as

$$\mathcal{E}(O) = d_A \mathrm{tr}_A[(O^T \otimes \mathbb{1})\rho_{AB}], \tag{246}$$

where the transpose denoted by $(\cdot)^T$ is taken in the standard basis. One can easily verify that the condition that $\rho_A = \mathbb{1}/d_A$ is connected to the fact that $\mathcal{E}$ is trace preserving.

This isomorphism can be exploited to derive uncertainty relations for quantum channels as corollaries from uncertainty relations for states, and vice versa. This point was emphasized by Coles *et al.* (2011). For example, if one has an uncertainty relation for bipartite states ρ_{AB}, such as Eq. (165), then one can apply this relation to the state in Eq. (245) in order to obtain an uncertainty relation for channels.

Specifically, note that if Alice measures observable $\mathbb{Z}$ on system A in Fig. 11(a) and obtains outcome $|\mathbb{Z}^z\rangle\langle\mathbb{Z}^z|$, then the state corresponding to the transpose $|\mathbb{Z}^z\rangle\langle\mathbb{Z}^z|^T$ will be sent through the channel $\mathcal{E}$. In other words,

$$\frac{1}{d}|\mathbb{Z}^z\rangle\langle\mathbb{Z}^z|^T = \mathrm{tr}_A[(|\mathbb{Z}^z\rangle\langle\mathbb{Z}^z| \otimes \mathbb{1})|\Phi\rangle\langle\Phi|]. \tag{247}$$

This implies that the Holevo quantity $\chi(\mathcal{E}, \mathbb{Z}^T)$ can be thought of as a classical-quantum mutual information as

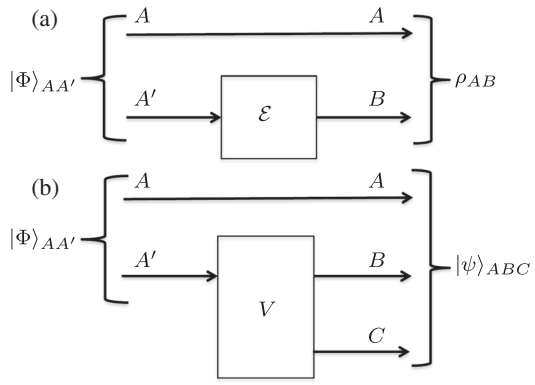


FIG. 11. How to convert the dynamical evolution of a system into (a) a bipartite mixed state or (b) a tripartite pure state.

$$\chi(\mathcal{E}, \mathbb{Z}^T) = I(Z{:}B) = \log d - H(Z|B), \tag{248}$$

where $\mathbb{Z}^T = \{|\mathbb{Z}^z\rangle\langle\mathbb{Z}^z|^T\}$, and the right-hand side is evaluated for the state

$$\rho_{ZB} = \sum_z |z\rangle\langle z| \otimes \mathrm{tr}_A[(|\mathbb{Z}^z\rangle\langle\mathbb{Z}^z| \otimes \mathbb{1}_B)\rho_{AB}] \tag{249}$$

$$= \sum_z \frac{1}{d}|z\rangle\langle z| \otimes \mathcal{E}(|\mathbb{Z}^z\rangle\langle\mathbb{Z}^z|^T). \tag{250}$$

Using Eq. (248), one can verify that the channel uncertainty relation (241) is a corollary of the bipartite state uncertainty relation, either (165) or (235).

3. Tripartite formulation

One can formulate uncertainty relations for a dynamic tripartite scenario where Alice sends the $\mathbb{Z}$ states over quantum channel $\mathcal{E}$ to Bob or the $\mathbb{X}$ states over the *complementary* quantum channel $\mathcal{F}$ to Charlie. The relationship between a channel and its complementary channel can be seen via the Stinespring dilation (Stinespring, 1955), in which one writes the channel in terms of an isometry V that maps $A \to BC$, namely,

$$\mathcal{E}(O) = \mathrm{tr}_C[VOV^\dagger], \tag{251}$$

$$\mathcal{F}(O) = \mathrm{tr}_B[VOV^\dagger]. \tag{252}$$

Analogous to Eq. (245), we consider the tripartite pure state defined by

$$|\psi\rangle_{ABC} = (\mathbb{1} \otimes V)|\Phi\rangle. \tag{253}$$

This mapping is depicted in Fig. 11(b). The tripartite uncertainty relations presented in Sec. IV.E can then be applied to the state $|\psi\rangle_{ABC}$ in Eq. (253) in order to derive uncertainty relations for complementary quantum channels. For example, Coles *et al.* (2011) read Eq. (206) in this way to obtain

$$\chi(\mathcal{E}, \mathbb{X}) + \chi(\mathcal{F}, \mathbb{Z}) \le \log(d^2 c), \tag{254}$$

for two orthonormal bases $\mathbb{X}$ and $\mathbb{Z}$. This relation implies that if Alice can send the $\mathbb{Z}$ states well to Charlie over the channel $\mathcal{F}$, then Bob cannot distinguish very well the outputs of the channel $\mathcal{E}$ associated with Alice sending a complementary set of states $\mathbb{X}$.

V. POSITION-MOMENTUM UNCERTAINTY RELATIONS

As discussed in Sec. I, the first precise statement of the uncertainty principle was formulated for position and momentum measurements. Namely, Kennard (1927) showed that for all states (with $\hbar = 1$)

$$\sigma(Q) \cdot \sigma(P) \ge \tfrac{1}{2}, \tag{255}$$

where $\sigma(Q)$ denotes the standard deviation of the probability density $\Gamma_Q(q)$ when measuring the position Q, and similarly for $\sigma(P)$ when measuring the momentum P.

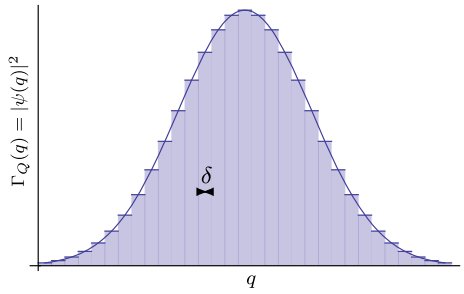


FIG. 12. Gaussian wave packet in position space with $\Gamma_Q(q)$ as in Eq. (256), as well as the finite resolution discretization from Eq. (260) in intervals of size δ.

Example 30. Consider Gaussian wave packets (see Fig. 12) with position probability density[23]

$$\Gamma_Q(q) = \frac{1}{\sqrt{2\pi\sigma^2}} \cdot \exp\left(-q^2 \cdot \frac{1}{2\sigma^2}\right), \tag{256}$$

and corresponding momentum probability density

$$\Gamma_P(p) = \sqrt{\frac{2\sigma^2}{\pi}} \cdot \exp\left(-p^2 \cdot 2\sigma^2\right). \tag{257}$$

It is then straightforward to check that these achieve equality in Eq. (255) and hence minimize the uncertainty in terms of the product of the two standard deviations.

In contrast to Kennard's formulation (255), the relations developed in Secs. III and IV are phrased in terms of entropy measures and apply to finite-dimensional systems (whereas position and momentum measurements can be modeled only on infinite-dimensional spaces). In this section we review entropic uncertainty relations with and without a memory system for position and momentum measurements.[24] We discussed applications to continuous variable quantum cryptography later in Sec. VI.B.5.

A. Entropy for infinite-dimensional systems

On a technical level, the position operator Q and the momentum operator P with the canonical commutation relation

$$[P, Q] = i\mathbb{1} \tag{258}$$

can be represented only as unbounded operators on infinite-dimensional spaces. Hence, we need to extend our setup from finite-dimensional Hilbert spaces to separable Hilbert spaces A with $\dim(A) = \infty$. However, quantum states can still be represented as linear, positive semidefinite operators. Hence, we just keep the notation the same as for finite-dimensional spaces without going into any mathematical details. We start with describing how to define entropy for infinite-dimensional systems.

1. Shannon entropy for discrete distributions

Imagine a finite resolution detector that measures the position Q by indicating in which interval

$$\mathcal{I}_{k;\delta} := (k\delta, (k+1)\delta] \quad (k \in \mathbb{Z}) \tag{259}$$

of size $\delta > 0$ the value q falls. This defines a discrete probability distribution Γ_{Q_δ} with infinitely many elements. If the initial state is described by a pure state wave function $|\psi(q)\rangle_Q$, we get $\{\Gamma_{Q_\delta}(k)\}_{k\in\mathbb{Z}}$ with

$$\Gamma_{Q_\delta}(k) = \int_{k\delta}^{(k+1)\delta} |\psi(q)|^2 dq. \tag{260}$$

We then define the Shannon entropy of Γ_{Q_δ} in the usual way as

$$H(Q_\delta) := -\sum_{k=-\infty}^{\infty} \Gamma_{Q_\delta}(k) \log \Gamma_{Q_\delta}(k). \tag{261}$$

Despite the fact that there are now infinitely many terms in the sum, $H(Q_\delta)$ keeps many of the properties of its finite-dimensional analog. In particular, $H(Q_\delta) \geq 0$ and the Shannon entropy can still be thought of as an information measure.

2. Shannon entropy for continuous distributions

The differential Shannon entropy is defined in the limit of infinitely small interval size $\delta \to 0$,

$$h(Q) := \lim_{\delta\to 0}[H(Q_\delta) + \log\delta] \tag{262}$$

$$= \lim_{\delta\to 0}\left(-\sum_{k=-\infty}^{\infty} \Gamma_{Q_\delta}(k) \log \frac{\Gamma_{Q_\delta}(k)}{\delta}\right). \tag{263}$$

The term $H(Q_\delta)$ scales with the interval $\delta \to 0$ and hence the normalization in Eq. (262). This makes the differential Shannon entropy an entropy density. There is also a closed formula for the differential Shannon entropy [at least when $\Gamma_Q(q)$ is continuous],

$$h(Q) = -\int dq \Gamma_Q(q) \log \Gamma_Q(q), \tag{264}$$

where $\Gamma_Q(q)$ denotes the probability density when measuring the position Q. For the momentum probability density $\Gamma_P(p)$ we define the discrete and differential Shannon entropy in the same way. Since probability densities can be larger than 1, not all of the properties of discrete Shannon entropy carry over. For example the differential Shannon entropy can be negative.

Example 31. For Gaussian wave packets as in Eqs. (256) and (257) we have

[23] In Sec. V, we use Γ instead of P for probability distributions since the momentum operator is already denoted by P.

[24] Entropic uncertainty relations for completely general quantum systems described by von Neumann algebras and measurements described by measure spaces are also studied in the literature (Frank and Lieb, 2013a; Furrer *et al.*, 2014).

$$h(Q) = \frac{1}{2}\log(2\pi e\sigma^2) \quad \text{and} \quad h(P) = \frac{1}{2}\log\frac{\pi e}{2\sigma^2}. \tag{265}$$

By inspection we find that $h(Q) < 0$ for σ sufficiently small and $h(P) < 0$ for σ sufficiently large.

Nevertheless the uncertainty principle can still be expressed in terms of differential Shannon entropies.

B. Differential relations

Extending the work of Everett (1957) and Hirschman (1957), Białynicki-Birula and Mycielski (1975) and independently Beckner (1975) showed for position and momentum measurements Q and P, respectively, that

$$h(P) + h(Q) \geq \log(e\pi). \tag{266}$$

We emphasized that Eq. (266) holds even though either one of the two differential Shannon entropies on the left-hand side can become negative. As in Kennard's relation (255) Gaussian wave packets again minimize the uncertainty and lead to equality in Eq. (266). This shows that the relation is tight. It is shown in Sec. II the entropic relation (266) also implies Kennard's relation (255) and is therefore stronger.

Recently alternative bounds were shown by Frank and Lieb (2012), Hall and Wiseman (2012), and Rumin (2012). In particular, extending the work of Beckner (1975), Hall (1999), and Rumin (2011), Frank and Lieb (2012) showed that

$$h(Q) + h(P) \geq \log(2\pi) + H(\rho_A), \tag{267}$$

where

$$H(\rho_A) \coloneqq -\mathrm{tr}[\rho_A \log \rho_A] \tag{268}$$

denotes the von Neumann entropy of the infinite-dimensional input state before any measurement was performed. We note that in contrast to the differential Shannon entropy, the von Neumann entropy is always non-negative since there is no regularization in its definition (even for infinite-dimensional systems). In Eq. (267) the state-independent bound $\log(2\pi) \leq \log(e\pi)$ is worse than in Eq. (266), but interestingly Eq. (267) becomes an equality for a thermal state in the infinite temperature limit (Hall, 1999; Frank and Lieb, 2012). Hence, Eq. (267) is also tight if we insist on having the von Neumann entropy $H(\rho_A)$ on the right-hand side.

C. Finite-spacing relations

It was argued in the literature that ideal position and momentum measurements can effectively never be performed because every detector has a finite accuracy. We can then ask in what other than a purely mathematical sense do Eqs. (266) and (267) express the uncertainty principle?[25] Certainly a more operational way to express uncertainty is in terms of the discrete Shannon entropy as defined in Eq. (261). A series of works (Partovi, 1983; Białynicki-Birula, 1984; Rojas González, Vaccaro, and Barnett, 1995; Rudnicki, 2011; Rudnicki, Walborn, and Toscano, 2012) established that for measurements with finite spacing δ_q for the position and finite spacing δ_p for the momentum we have

$$H(Q_\delta) + H(P_\delta) \geq \log(2\pi) - \log\left[\delta_q\delta_p \cdot S_0^{(1)}\left(1, \frac{\delta_q\delta_p}{4}\right)^2\right], \tag{269}$$

where $S_0^{(1)}(\cdot,\cdot)$ denotes the zeroth radial prolate spheroidal wave function of the first kind (Slepian and Pollak, 1961). This way of expressing the uncertainty principle has the advantage that the discrete Shannon entropy is always non-negative and has a clear information-theoretic interpretation. As seen later, it is the discrete formulation of the uncertainty principle that becomes relevant for applications in continuous variable quantum cryptography (see Secs. V.E and VI.B.5).

Interestingly Eq. (269) is not tight for general $\delta > 0$ since we also know that (Białynicki-Birula, 1984)

$$H(Q_{\delta q}) + H(P_{\delta p}) \geq \log(e\pi) - \log(\delta_q\delta_p), \tag{270}$$

which becomes tighter for $\delta \to 0$ (see Fig. 13). Rudnicki (2015) employed a majorization-based approach along the lines of Sec. III.I to improve on Eqs. (269) and (270) for large spacing. However, this does not yield a closed formula and we refer to Rudnicki (2011, 2015) for a discussion of tightness and a more detailed comparison. We further comment on this issue in Sec. V.D after extending Eqs. (266) and (269) to a quantum memory system.

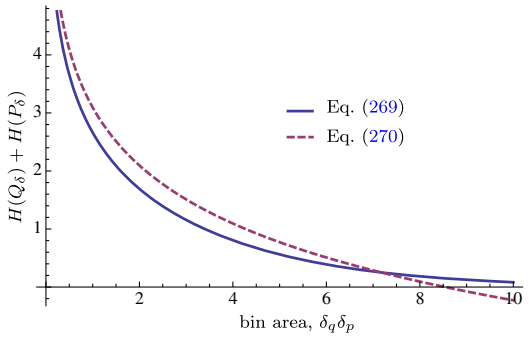


FIG. 13. Comparison of the lower bounds in Eqs. (269) and (270) on the uncertainty generated by the finite-spacing position and momentum measurements Q_δ, P_δ as in Eq. (260). Note that the latter bound becomes negative and hence trivial for larger spacings $\delta_q\delta_p \gtrsim 8.5$.

D. Uncertainty given a memory system

For finite-dimensional systems we can write the conditional von Neumann entropy of bipartite quantum states ρ_{AB} as $H(A|B) = H(AB) - H(B)$. However, for infinite-dimensional systems this is in general not a sensible notion of conditional entropy. This is because for some states both terms $H(AB)$ and $H(B)$ can become infinite even though the entropy of A is

[25]This criticism also applies to Kennard's relation (255) and a finite-spacing version thereof was derived by Rudnicki, Walborn, and Toscano (2012).

finite and hence the conditional entropy should also remain finite.

Example 32. Consider a bipartite system with A one qubit and B composed of infinitely many qubits indexed by $k \in \mathbb{N}$. Let $|\psi\rangle_{AB_k}$ be maximally entangled between A and the kth qubit on B, and let $|\phi^k\rangle_{B/B_k}$ be some pure states on B (except B_k) such that $\langle\phi^k|\phi^{k'}\rangle = \delta_{kk'}$. Now, for a probability distribution $p_k \propto 1/k(\log k)^2$ for $k > 2$ (Wehrl, 1978), the bipartite quantum state

$$\rho_{AB} = \sum_k p_k |\psi\rangle\langle\psi|_{AB_k} \otimes |\phi^k\rangle\langle\phi^k|_{B/B_k} \tag{271}$$

has

$$H(AB) = \infty \quad \text{and} \quad H(B) = \infty. \tag{272}$$

However, any sensible definition of conditional entropy for this state ρ_{AB} should give $H(A|B) = -1$.[26]

Observe that the conditional entropy of finite-dimensional classical-quantum states ρ_{XB} as in Eq. (136) can be rewritten in terms of the relative entropy (Umegaki, 1962),

$$D(\rho\|\sigma) := \mathrm{tr}[\rho(\log\rho - \log\sigma)], \tag{273}$$

as

$$H(X|B) = -\sum_x D[P_X(x)\rho_B^x\|\rho_B]. \tag{274}$$

Furrer *et al.* (2014) pointed out that Eq. (274) can be lifted to

$$H(Q_\delta|B) := -\sum_{k=-\infty}^{\infty} D(\rho_B^{k;\delta}\|\rho_B), \tag{275}$$

where $\rho_B^{k;\delta}$ denotes the (subnormalized) marginal state on B when the position Q is measured in $\mathcal{I}_{k;\delta}$, i.e., $P_{Q_\delta}(k) := \mathrm{tr}[\rho_B^{k;\delta}]$ is the probability to measure in $\mathcal{I}_{k;\delta}$.

1. Tripartite quantum memory uncertainty relations

With Eq. (275) as the definition for classical-quantum entropy Furrer *et al.* (2014) found

$$H(Q_{\delta q}|B) + H(P_{\delta p}|C) \geq \log(2\pi) - \log\left[\delta_q\delta_p \cdot S_0^{(1)}\left(1, \frac{\delta_q\delta_p}{4}\right)^2\right]. \tag{276}$$

This is the extension of Eq. (269) to quantum memories and likewise not tight. By taking the limit $\delta \to 0$ we find the differential quantum conditional entropy

$$h(Q|B) := \lim_{\delta\to 0}[H(Q_\delta|B) + \log\delta] \tag{277}$$

$$= \int dq D(\rho_B^q\|\rho_B), \tag{278}$$

where the second equality holds under a particular finiteness assumption (Furrer *et al.*, 2014). With Eq. (276) we then immediately find the extension of Eq. (266) to quantum memories,

$$h(Q|B) + h(P|C) \geq \log(2\pi). \tag{279}$$

Example 33. For the EPR state on AB (or likewise AC) in the limit of perfect correlations Eq. (279) becomes an equality. For finite squeezing strength $r = \mathrm{arccosh}(\nu)/2$ the EPR state is a Gaussian state with covariance matrix

$$\Gamma_{AB}(\nu) = \frac{1}{2}\begin{pmatrix} \nu\mathbb{1}_2 & \sqrt{\nu^2-1}Z_2 \\ \sqrt{\nu^2-1}Z_2 & \nu\mathbb{1}_2 \end{pmatrix} \tag{280}$$

with

$$\mathbb{1}_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad Z_2 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{281}$$

See Weedbrook *et al.* (2012) for more details about Gaussian quantum information theory. The left-hand side of Eq. (279) for this state generated by $\Gamma_{AB}(\nu)$ is then calculated to be (Furrer *et al.*, 2014)

$$h(Q|B) + h(P) = \log(e\pi\nu) - \frac{\nu+1}{2}\log\left(\frac{\nu+1}{2}\right) + \frac{\nu-1}{2}\log\left(\frac{\nu-1}{2}\right), \tag{282}$$

which converges to $\log(2\pi)$ for $\nu \to \infty$. In Fig. 14 we plot Eq. (282) as a function of the squeezing strength $r = \frac{1}{2}\mathrm{arccosh}(\nu)$:

(1) For $r = 0$ the system B is uncorrelated and we have the lower bound $h(Q) + h(P) \geq \log(e\pi)$ as in Eq. (266).
(2) For $r > 0$ we have to take the quantum memory B into account and only the lower bound $h(Q|B) + h(P) \geq \log(2\pi)$ from Eq. (279) holds.
(3) For $r \to \infty$ we get maximal correlations and the bound (279) becomes an equality.

We note that in typical experiments for applications (see Sec. VI.B.5) a squeezing strength of $r \approx 1.5$ is achievable (Eberle, Händchen, and Schnabel, 2013). For this the lower bound (279) is already very tight.

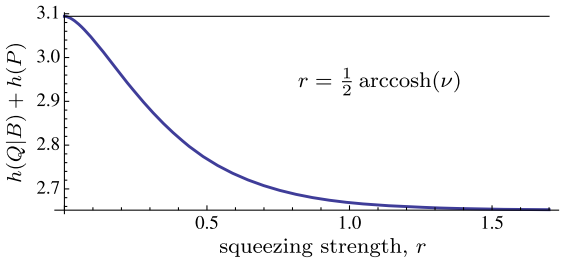


FIG. 14. The uncertainty $h(Q|B) + h(P)$ of the EPR state from example 33 in terms of the squeezing strength r.

[26] See Kuznetsova (2011) for an extended discussion.

The state-independent bound in Eq. (279) is $\log(2\pi)$, whereas it is $\log(e\pi)$ for the case without quantum memory in Eq. (266). Hence, in contrast to the finite-dimensional case, a quantum memory reduces the state-independent uncertainty limit. This is because for the approximate EPR state there exists a gap between the accessible classical correlation and the classical-quantum correlation. That is, even when minimized over all measurements Q_B on B, we have $h(Q|Q_B) - h(Q|B) \approx \log(e/2)$.

2. Bipartite quantum memory uncertainty relations

Similarly as for finite-dimensional systems it is possible to formulate uncertainty relations with quantum memory in a bipartite form. For continuous position and momentum measurements Frank and Lieb (2013a) showed that

$$h(Q|B) + h(P|B) \geq \log(2\pi) + H(A|B)_\rho. \tag{283}$$

This is the extension of Eq. (267) to a quantum memory system. However, we note that Eq. (283) only holds if all the terms appearing in $H(A|B) = H(AB) - H(B)$ are finite (which is in general too restrictive).[27]

3. Mutual information approach

A conceptually different approach was taken by Hall (1995), where the uncertainty relative to a memory system is quantified in terms of mutual information instead of conditional entropy (see Sec. IV.F for a general discussion). Similarly as for the conditional entropy in Eq. (275), mutual information for classical-quantum states is most generally defined in terms of the relative entropy in Eq. (273),

$$I(Q_\delta{:}B) \coloneqq \sum_{k=-\infty}^{\infty} [D(\rho_B^{k;\delta}\|\rho_B) + H(B)_{\rho^{k;\delta}}]. \tag{284}$$

In contrast to entropy, however, the mutual information stays finite when taking the limit $\delta \to 0$,

$$I(Q{:}B) \coloneqq \lim_{\delta\to 0} I(Q_\delta{:}B). \tag{285}$$

Hence, no regularization in terms of the interval size δ is taken. For classical memories M it was shown that (Hall, 1995)

$$I(Q{:}M) + I(P{:}M) \leq 1 + \log\sigma(Q) + \log\sigma(P). \tag{286}$$

It is an open question to find a generalization that also holds for quantum memories. This would be in analogy to what is known for finite-dimensional systems (see Sec. IV.F.4).

E. Extension to min- and max-entropies

As for finite-dimensional systems, entropic uncertainty relations like Eqs. (266) and (269) cannot be shown only for the Shannon entropy, but also more generally for pairs of Rényi entropies (Białynicki-Birula, 2006, 2007; Rudnicki, Walborn, and Toscano, 2012; Rastegin, 2015c). Here we focus on a special case that is important for applications in continuous variable quantum cryptography (see Sec. VI.B.5). We study relations in terms of the Rényi entropy of order ∞ and its dual quantity the Rényi entropy of order $1/2$. These are exactly the min- and max-entropies, respectively.

1. Finite-spacing relations

Following the finite resolution detector picture as in Eqs. (259) and (260), the conditional min-entropy is defined as

$$H_{\min}(Q_\delta|B) \coloneqq -\log p_{\text{guess}}(Q_\delta|B). \tag{287}$$

Here we have the optimal guessing probability as in Eq. (137),

$$p_{\text{guess}}(X|B) \coloneqq \sup_{\mathbb{X}_B}\left\{\sum_{k=-\infty}^{\infty} \Gamma_{Q_\delta}(k)\text{tr}[\mathbb{X}_B^k \rho_B^{k;\delta}] : \mathbb{X}_B \text{ POVM on } B\right\}. \tag{288}$$

In analogy to the finite-dimensional case, the min-entropy quantifies the uncertainty of the classical register Q_δ from the perspective of an observer with access to the quantum memory B. The conditional max-entropy is given by

$$H_{\max}(Q_\delta|B) \coloneqq \log F_{\text{dec}}(Q_\delta|B), \tag{289}$$

where we have the optimal decoupling fidelity

$$F_{\text{dec}}(Q_\delta|B) \coloneqq \sup\left\{\left(\sum_{k=-\infty}^{\infty} \sqrt{F(\rho_B^{k;\delta}, \sigma_B)}\right)^2 : \sigma_B \text{ state on } B\right\}. \tag{290}$$

The decoupling fidelity is a measure of how much information the quantum memory B contains about the classical register Q_δ.[28] For these definitions Furrer *et al.* (2014) showed

$$H_{\min}(Q_\delta|B) + H_{\max}(P_\delta|C) \geq \log(2\pi) - \log\left[\delta_q\delta_p \cdot S_0^{(1)}\left(1, \frac{\delta_q\delta_p}{4}\right)^2\right], \tag{291}$$

as well as the same relation with Q_δ and P_δ interchanged. We note that the special case with trivial quantum memories B, C was already shown by Rudnicki, Walborn, and Toscano (2012). Furrer *et al.* (2014) showed that Eq. (291) is tight for any spacing $\delta > 0$ even in the absence of any correlations (i.e., there exist states for which the relation becomes an equality). Note that this is in contrast to the situation for the Shannon entropy, where neither Eqs. (269), (270), nor (276) are tight.

[27] This restriction is connected with the question about a sensible notion of conditional entropy for fully quantum states (Kuznetsova, 2011).

[28] For finite-dimensional systems Eq. (289) is equivalent to the max-entropy as defined in Eq. (155); see König, Renner, and Schaffner (2009) and Furrer *et al.* (2014).

2. Differential relations

For the differential version we take the limit $\delta \to 0$,

$$h_{\min}(Q|B) \coloneqq \lim_{\delta\to 0}[H_{\min}(Q_\delta|B) + \log\delta], \tag{292}$$

and similarly for $h_{\max}(Q|B)$.[29] We then find the uncertainty relation (Furrer *et al.*, 2014)

$$h_{\min}(Q|B) + h_{\max}(P|C) \geq \log(2\pi) \tag{293}$$

as well as the same relation with Q and P interchanged. Białynicki-Birula (2006) showed that Eq. (293) becomes an equality for pure Gaussian states as in Eqs. (256) and (257). Note that this implies, in particular, that the unconditional special case

$$h_{\min}(Q) + h_{\max}(P) \geq \log(2\pi) \tag{294}$$

is tight. Hence, the optimal state-independent constant is $\log(2\pi)$ for the min- and max-entropies, whereas the optimal constant for the Shannon entropy in Eq. (266) is $\log(e\pi)$.

F. Other infinite-dimensional measurements

As a multidimensional extension of Eq. (266), Huang (2011) showed that for any measurements of the form

$$A = \sum_{i=1}^{n} a_i Q_i + a_i' P_i, \qquad B = \sum_{i=1}^{n} b_i Q_i + b_i' P_i, \tag{295}$$

with $a_i, a_i', b_i, b_i' \in \mathbb{R}$ we have that

$$h(A) + h(B) \geq \log(e\pi) + \log|[A,B]|. \tag{296}$$

Huang (2011) also showed that for any measurement pair A, B as in Eq. (295) there exist states for which Eq. (296) becomes an equality.

Moreover, the techniques for deriving position-momentum uncertainty relations can also be applied to other complementary observable pairs that are modeled on infinite-dimensional Hilbert spaces. For example, for a particle on a circle we have the position angle φ and the conjugate angular momentum observable L_z. Consider a measurement device that tells either in which of

$$M \coloneqq 2\pi/\delta_\varphi \quad \text{bins of size } \delta_\varphi \tag{297}$$

the particle is in or the exact value of the angular momentum L_z. We get a discrete probability distribution P_{φ_δ} for the angle defined similarly as in Eq. (260), as well as a discrete probability distribution P_{L_z} over the L_z eigenstates. Improving on the earlier work of Partovi (1983), Białynicki-Birula (1984) showed that

$$H(\varphi_\delta) + H(L_z) \geq \log M. \tag{298}$$

By inspection Eq. (298) becomes an equality for any eigenstate of the L_z observable. The relation was also extended to two angles φ and θ and the corresponding pair of observables L_z and L^2 (Białynicki-Birula and Madajczyk, 1985).

Another observable pair is the number N and the phase Φ for the harmonic oscillator. Hall (1993) showed that

$$H(N) + h(\Phi) \geq \log 2\pi, \tag{299}$$

where $P_N(n)$ represents the probability distribution in the number basis $\{|n\rangle\}$, and the probability density in the phase basis is

$$P_\Phi(\phi) \coloneqq \frac{|\langle e^{i\phi}|\psi\rangle|^2}{2\pi} \quad \text{with} \quad |e^{i\phi}\rangle \coloneqq \sum_n e^{in\phi}|n\rangle \tag{300}$$

the Susskind-Glogower phase kets (which are not normalized).[30] This can also be seen as a special case of the results in Białynicki-Birula and Mycielski (1975). Equation (299) becomes an equality for number states. Furthermore, Hall (1994) also extended (299) to noisy harmonic oscillators degraded by Gaussian noise.

Finally, time-energy entropic uncertainty relations for systems with discrete energy spectra were discussed by Hall (2008).

VI. APPLICATIONS

A. Quantum randomness

Randomness is a crucial resource for many everyday information-processing tasks, ranging from online gambling to scientific simulations and cryptography. Randomness is a scarce resource since computers are designed to perform deterministic operations. Even more importantly classical physics is deterministic, meaning that every outcome of an experiment can in principle be predicted by an observer who has full knowledge of the initial state of the physical system and the operations that are performed on it. The study of pseudorandomness tries to circumvent this problem (Vadhan, 2012).

Quantum mechanics with its inherent nondeterminism allows us to consider a stronger notion of randomness, namely, randomness that is information-theoretically secure. Formally, we want to generate a random variable L that is uniformly distributed over all bit strings $\{0,1\}^\ell$ of a given length ℓ. Moreover, we want this random variable to be independent of any side information an observer might have, including information about the process that is used to calculate L and any random seeds that are used to prepare L. A classical-quantum product state

[29] Under some finiteness assumptions we have $h_{\max}(Q|B) = 2\log\sup\{\int dq\sqrt{F(\rho_B^q,\sigma_B)}:\sigma_B \text{ state on } B\}$ as well as $h_{\min}(Q|B) = -\log\sup\{\int dq\rho_B^q(\mathbb{X}_B^q):q\mapsto\mathbb{X}_B^q \text{ POVM on } B\}$.

[30] Because of the nonorthogonality of the phase kets $|e^{i\phi}\rangle$ there is no observable corresponding to the phase distribution $P_\Phi(\phi)$. This, however, will not concern us further since $P_\Phi(\phi)$ is well defined.

$$\pi_{LE} = \frac{1}{2^\ell} \sum_{i=1}^{2^\ell} |i\rangle\langle i|_L \otimes \pi_E \tag{301}$$

describes ℓ bits of uniform randomness that is independent of its environment or side information E. Often, the best we can hope for is to approximate such a state. Namely, we say that ρ_{ZE} describes a state where L is δ close to uniform on ℓ bits and independent of E if

$$\left\| \rho_{LE} - \frac{1}{2^\ell} \sum_{i=1}^{2^\ell} |i\rangle\langle i|_L \otimes \rho_E \right\|_{\mathrm{tr}} \leq \delta, \tag{302}$$

where $\| \cdot \|_{\mathrm{tr}}$ denotes the trace norm. This bound implies that L cannot be distinguished from a uniform and independent random variable with probability more than $\frac{1}{2}(1+\delta)$. This viewpoint is at the core of universally composable security frameworks (Canetti, 2001; Unruh, 2010), which ensure that a secret key satisfying this property can safely be employed in any cryptographic protocol requiring a secret key.

Entropic uncertainty relations can help us since they certify that the random variables resulting from a quantum measurement are uncertain and thus contain randomness. However, in order to extract approximately uniform and independent randomness we need an additional step, which we describe next.

1. The operational significance of conditional min-entropy

The importance of the min-entropy in cryptography is partly due to the following lemma, called the leftover hashing lemma (Mclnnes, 1987; Impagliazzo, Levin, and Luby, 1989; Impagliazzo and Zuckerman, 1989). Informally, it states that there exists a family of functions $\{f_s\}_s$, where $f_s \colon \mathcal{X} \to [2^\ell]$, called hash functions, such that the random variable $L = f_S(X)$, which results by applying the function f_S with S a seed chosen uniformly at random, is close to uniform and independent of S if the initial min-entropy is sufficiently large.

More formally, Renner (2005) and Renner and König (2005) showed the following result for the quantum case. There exists a family $\{f_s\}_s$ of hash functions such that for any classical-quantum state

$$\rho_{XE} = \sum_x P_X(x)|x\rangle\langle x|_X \otimes \rho_E^x \tag{303}$$

with $H_{\min}(X|E) \geq k$, the classical-quantum-classical state ρ_{LES} after applying f_S, namely,

$$\rho_{LES} = \sum_{s,x} \frac{P_X(x)}{|S|} |f_s(x)\rangle\langle f_s(x)|_L \otimes \rho_E^x \otimes |s\rangle\langle s|_S \tag{304}$$

describes a state where L is δ close to uniform on ℓ bits and independent of E and S with $\delta = 2^{(1/2)(\ell-k)}$.

The special case where the environment E is trivial was discussed extensively in the computer science literature (Vadhan, 2012). Since hashing is a classical process, one might expect that the physical nature of the side information is irrelevant and that a classical treatment is sufficient. However, this is not true in general. For example, the output of certain extractors may be partially known if side information about their input is stored in a quantum memory, while the same output is almost uniform conditioned on any classical side information.[31]

A generalization of this result is possible by considering a variation of the min-entropy, which is called ε-smooth min-entropy, and denoted $H_{\min}^\varepsilon(X|E)$, for a small $\varepsilon > 0$. This is defined by maximizing the min-entropy over states that are in a ball of radius ε around the state ρ.[32]

The generalized leftover hashing lemma (Renner, 2005; Tomamichel *et al.*, 2011) asserts that there exists a family $\{f_s\}_s$ such that for any state ρ_{XE} with $H_{\min}^\varepsilon(X|E) \geq k$, we find that $L = f_S(X)$ is $\varepsilon + \delta$ close to uniform and independent of E and S, with δ as defined previously.

The latter result is tight in the following sense. If $L = f_S(X)$ is ε close to uniform and independent from E and S for any family of functions $\{f_s\}_s$, then we must have $H_{\min}^{\varepsilon'}(X|E) \geq \ell$ with $\varepsilon' = \sqrt{2\varepsilon}$.

Because of this tightness result we are justified to say that the smooth min-entropy characterizes (at least approximately) how much uniform randomness can be extracted from a random source X that is correlated with its environment E.

2. Certifying quantum randomness

Note that we can certify randomness, if we can somehow conclude that $H_{\min}(X|E)$ is large. In principle, all entropic uncertainty relations that involve a quantum memory are suitable for this task, whenever we can verify the terms lower bounding the entropy. Tripartite uncertainty relations are especially suitable to this task, and the security of quantum key distribution below rests on our ability to make such estimates. For example, Vallone *et al.* (2014) specialized the uncertainty relation for min- and max-entropies in Eq. (222) to assert that

$$H_{\min}(X|E)_\rho \geq \log d - H_{\max}(Z), \tag{305}$$

where $\mathbb{X}$ and $\mathbb{Z}$ are mutually unbiased measurements on a d-dimensional Hilbert space. Here E is the environment of the measured system and the max-entropy $H_{\max}(Z) = H_{1/2}(Z)$ can be estimated using statistical tests, resulting in confidence about $H_{\min}(X|E)$. As discussed, the leftover hashing lemma now allows one to extract uniform randomness from X.

Miller and Shi (2014) derived a lower bound on an entropy difference instead of a conditional entropy. Assume that $\mathbb{X}$ and $\mathbb{Z}$ are complementary binary measurements on a qubit. Then the following relation holds:

$$H_\alpha(XB) - H_\alpha(B) \geq q(\alpha, \delta) \quad \text{for } \alpha \in (1, 2], \tag{306}$$

where δ is determined by the equality

$$\mathrm{tr}[\langle \mathbb{Z}^0 | \rho_{AB} | \mathbb{Z}^0 \rangle^\alpha] = \delta \mathrm{tr}[\rho_B^\alpha], \tag{307}$$

[31] See Gavinsky *et al.* (2009) for a concrete example and König and Renner (2011) for a more general discussion of this topic.

[32] See Tomamichel, Colbeck, and Renner (2010) for a precise definition of smooth min-entropy.

and q is a function satisfying $\lim_{\alpha\to 1} q(\alpha,\delta) = 1 - 2h(\delta)$. They then proceeded to use this result to bound the smooth min-entropy and apply the generalized leftover hashing lemma.

B. Quantum key distribution

The goal of a key distribution scheme is for two honest parties to agree on a shared key by communicating over a public channel in such a way that the key is secret from any potential adversary eavesdropping on the channel. Traditionally the two honest parties trying to share a key are called Alice and Bob and the eavesdropper is called Eve. By a simple symmetry argument it is evident that key distribution is impossible if only classical information is considered: Since Eve will hear all communication from Alice to Bob, at any point in the protocol she will have at least as much information about Alice's key as Bob—in particular, if Bob knows Alice's key then so does Eve.

Quantum key distribution (QKD) was first proposed by Bennett and Brassard (1984) and Ekert (1991) to get out of this impasse.[33] Since quantum information cannot be copied or cloned (Wootters and Zurek, 1982), the symmetry argument no longer applies when Alice and Bob are allowed to communicate over a quantum channel. Roughly speaking, the main idea is that whenever the eavesdropper interacts with the channel (for example, by performing a measurement on a particle), she will necessarily introduce noise in the quantum communication between Alice and Bob, which they can then detect and subsequently abort the protocol.

1. A simple protocol

We focus on a truncated version of Ekert's protocol (Ekert, 1991), which proceeds as follows.

Preparation: Alice and Bob share a maximally entangled two-qubit state using the public channel. Eve can coherently interact with the channel.

Measurement: They randomly agree (using the public channel) on either the basis $\mathbb{Z} = \{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ or $\mathbb{X} = \{|+\rangle\langle +|, |-\rangle\langle -|\}$, and measure their respective qubits in this basis. (These two steps are repeated many times.)

Parameter estimation: Alice announces her measurement results on a random subset of these rounds. If their measurement results agree on most rounds, they conclude that their correlations contain some secrecy and proceed to correct their errors and extract a secret key (we will not discuss this further here). If not, they abort the protocol.

2. Security criterion for QKD

To show security of QKD we thus need to show that the following two statements are mutually exclusive: (a) Alice's and Bob's measurement results agree in most rounds, and (b) Eve has a lot of information about Alice's or Bob's measurement outcomes.

Security of quantum key distribution against general attacks was first formally established by Mayers (1996, 2001) as well as Biham *et al.* (2000, 2006) and Shor and Preskill (2000). In all these security arguments, the complementarity or uncertainty principle is invoked in some form to argue that if Alice and Bob have large agreement on the qubits measured in one basis, then necessarily Eve's information about the bits measured in the complementary basis must be low.

In Sec. VI.B.3 we attempted to present the security argument in a concise and intuitive way, and for this purpose we adopt a notion of security—certifying that the raw key has high Shannon entropy—that has proven to be insufficient in practice. However, our ultimate goal is to extract a secret key and not to have a bit string with high Shannon entropy. This ultimately requires the use of different entropies and a postprocessing step in the protocol to distill a secret key. A discussion of these issues follows in Sec. VI.B.4.

Entropic uncertainty relations were first used in this context by Cerf *et al.* (2002) and Grosshans and Cerf (2004). In particular, Koashi (2006) established security by leveraging the Maassen-Uffink relation (31). However, entropic uncertainty relations with quantum memory provide a more direct avenue to formalize security arguments for QKD, as we see in the following.

3. Proof of security via an entropic uncertainty relation

(a) Single round. We broadly follow here an argument outlined by Berta *et al.* (2010). First note that during the preparation step the eavesdropper might interfere and we will thus not know if Alice and Bob will indeed share a maximally entangled state after the preparation step is complete. However, without loss of generality we may assume that Alice (A), Bob (B), and Eve (E) share an arbitrary state ρ_{ABE} after the preparation step, where A and B are qubits and E is any quantum system held by Eve [see Fig. 15(a)].

Let Θ be a binary register in a fully mixed state that determines if the qubits are to be measured in the basis $\mathbb{X}$ or $\mathbb{Z}$ and let Y denote the output of Alice's measurement. Then we can write $H(Y|B\Theta) = (1/2)H(X|B) + (1/2)H(Z|B)$ and similarly $H(Y|E\Theta) = (1/2)H(X|E) + (1/2)H(Z|E)$. Thus, the tripartite entropic uncertainty principle with quantum memory (206) can be cast into the form

$$H(Y|E\Theta) + H(Y|B\Theta) \geq q_{\mathrm{MU}} = 1, \tag{308}$$

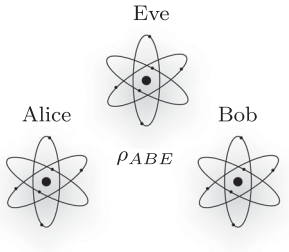
where we have that $q_{\mathrm{MU}} = 1$ for the measurements $\mathbb{X}$ and $\mathbb{Z}$. The entropies are evaluated for the state $\rho_{Y\Theta BE}$ after the measurement on Alice's qubit is performed.

Next we perform Bob's measurement, which yields an estimate $\hat{Y}$ of Y. The data-processing inequality (C6) implies that $H(Y|B\Theta) \leq H(Y|\hat{Y})$, and thus we conclude that $H(Y|E\Theta) \geq 1 - H(Y|\hat{Y})$. This ensures that Eve's uncertainty, in terms of von Neumann entropy, of Alice's measurement outcome is large as long as the conditional entropy $H(Y|\hat{Y})$ is small [see Fig. 15(b)]. This is a quantitative expression of the security criterion.[34]

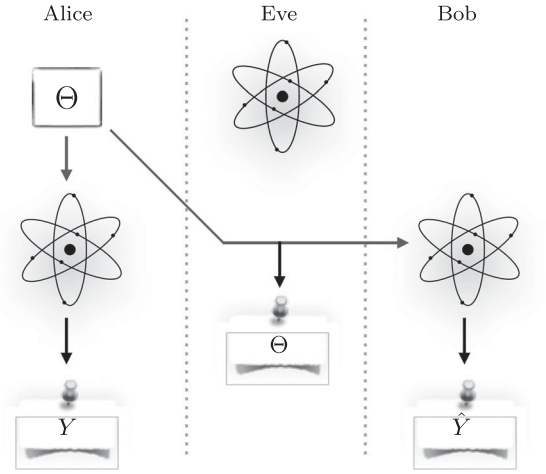
Example 34. If Alice and Bob's measurement outcomes agree with high probability, let us say with probability $1 - \delta$,

[33] See Scarani *et al.* (2009) for a recent review.

[34] Note that in practice we need a stronger statement, namely, a bound on the min-entropy. This is discussed in Sec. VI.B.4.



(a) Preparation phase



(b) Measurement phase: Alice and Bob measure their quantum system in the basis indicated by Θ to recover Y and $\hat{Y}$, respectively. Eve stores Θ and keeps her quantum memory intact. The uncertainty relation is applied to the resulting state $\rho_{Y\hat{Y}E\Theta}$.

FIG. 15. Preparation and measurement phase of the QKD protocol described in Sec. VI.B.1.

then $H(Y|\hat{Y})$ evaluates to $h_{\text{bin}}(\delta) = \delta \log(1/\delta) + (1-\delta)\log[1/(1-\delta)]$. Hence, we find that

$$H(Y|E\Theta) \geq 1 - h_{\text{bin}}(\delta), \tag{309}$$

which is positive as long as δ is strictly less than 50%.

(b) Multiple rounds. The protocol extends over multiple rounds and we can repeat the argument for each round individually and then attempt to add up the resulting entropies, but it is much more convenient to use a stronger uncertainty relation that describes the situation for multiple rounds directly.

For this purpose, let us model the situation after Alice and Bob have exchanged n qubits but before they measure them. This is a hypothetical situation since in the actual protocol Alice and Bob measure their qubits after every round. However, we can always imagine that Alice and Bob delay their measurement since Eve's strategy cannot depend on the timing of their measurement. After the exchange Alice and Bob each hold n qubits in systems $A^n = A_1A_2\cdots A_n$ and $B^n = B_1B_2\cdots B_n$, respectively. This is described by an arbitrary state $\rho_{A^nB^nE}$, where E is any quantum system held by the eavesdropper. Again, we model the random measurement choice using a register, a bit string $\Theta^n = (\Theta_1, \Theta_2, \ldots, \Theta_n)$ of length n in a fully mixed state, where Θ_i determines the choice of measurement on the systems indexed by i. Analogously, we store the measurement outcomes on Alice's system in a bit string $Y^n = (Y_1, Y_2, \ldots, Y_n)$ and on Bob's system in a bit string $\hat{Y}^n = (\hat{Y}_1, \hat{Y}_2, \ldots, \hat{Y}_n)$.

The crucial observation is that the tripartite uncertainty principle in Eq. (206) implies that

$$H(X_1X_2Z_3X_4\cdots X_{n-1}Z_n|E) + H(Z_1Z_2X_3Z_4\cdots Z_{n-1}X_n|B) \geq n, \tag{310}$$

where we made sure that all n systems are measured in the opposite basis in the two terms, and used that $\log(1/c^n) = n$. A similar averaging argument for the one round case and the data-processing inequality (C6) then reveal the bounds

$$H(Y^n|E\Theta^n) + H(Y^n|\hat{Y}^n) \geq H(Y^n|E\Theta^n) + H(Y^n|B^n\Theta^n) \geq n. \tag{311}$$

Hence, Eve's uncertainty (in terms of von Neumann entropy) of the measurement outcome Y^n increases linearly in the number of rounds. Notably, this is true without assuming anything about the attack. In particular, the state $\rho_{A^nB^nE}$ after preparation but before the uncertainty principle is applied does not need to have any particular structure and is assumed to be arbitrary.

4. Finite size effects and min-entropy

So far we have argued that security of QKD is ensured if Eve's uncertainty of the key expressed in terms of the von Neumann entropy is large. This might be a reasonable *ad hoc* criterion, but more operationally what we want to say is that a key is secure if it can be safely used in any other protocol, for example, one-time pad encryption that requires a secret key. This leads to the notion of composable security, first studied by Renner (2005) in the context of QKD. It turns out that in order to achieve composable security for a key of finite length, it is not sufficient to consider Eve's uncertainty in terms of the von Neumann entropy. Instead, it is necessary to ensure that the smooth min-entropy of the measurement results is large (Renner and König, 2005), so that we can extract a secret key, i.e., uniform randomness that is independent of the eavesdropper's memory. (Recall the discussion of randomness in Sec. VI.A.) Thus, instead of the inequality (310) involving von Neumann entropies, we want to apply a generalization of the Maassen-Uffink uncertainty relation with quantum memory (221). This leads to the following relation (Tomamichel and Renner, 2011):

$$H^{\varepsilon}_{\text{min}}(Y^n|E\Theta^n) + H^{\varepsilon}_{\text{max}}(Y^n|\hat{Y}^n) \geq n, \tag{312}$$

where $H^{\varepsilon}_{\text{min}}$ and $H^{\varepsilon}_{\text{max}}$ denote the smooth min- and max-entropies, variations of the min- and max-entropies (that we will not discuss further here). Hence, in order to ensure security it is sufficient to estimate the smooth max-entropy $H^{\varepsilon}_{\text{max}}(Y^n|\hat{Y}^n)$. This can be done by a suitable parameter estimation procedure as shown by Tomamichel *et al.* (2012).

5. Continuous variable QKD

Quantum information processing with continuous variables (Weedbrook *et al.*, 2012) offers an interesting and practical alternative to finite-dimensional systems. Here we discuss a particular variation of the above QKD protocol, where Alice and Bob measure the quadrature components of an electromagnetic field and then extract a secret key from the correlations contained in the resulting continuous variables.

If Alice and Bob share a squeezed Gaussian state, Furrer *et al.* (2012) showed that the security of such protocols can be shown rigorously using entropic uncertainty relations, including finite size effects. For this purpose, it is convenient to employ a smoothed extension of Eq. (291) as first shown by Furrer, Aberg, and Renner (2011). This yields

$$H_{\min}^{\varepsilon}(Y^n|E\Theta^n) + H_{\max}^{\varepsilon}(Y^n|\hat{Y}^n) \geq n \log\left[\frac{2\pi}{\delta^2}\cdot S_0^{(1)}\left(1,\frac{\delta^2}{4}\right)^{-2}\right], \tag{313}$$

where Y_i is the outcome of the quadrature measurement in the basis (position or momentum) specified by Θ_i discretized with bin size δ. See Gehring *et al.* (2015) for an implementation.

C. Two-party cryptography

In this section we discuss applications of entropic uncertainty relations to cryptographic tasks between two mutually distrustful parties (traditionally called Alice and Bob). This setup is in contrast to quantum key distribution where Alice and Bob do trust each other and only a third party is eavesdropping. Typical tasks for two-party cryptography are bit commitment, oblivious transfer, or secure identification.

It turns out, however, that even using quantum communication it is possible only to obtain security if we make some assumptions about the adversary (Lo, 1997; Lo and Chau, 1997; Mayers, 1997). What makes this problem harder is that unlike in QKD where Alice and Bob trust each other to check on any eavesdropping activity, here every party has to fend for himself. Nevertheless, since tasks such as secure identification are of great practical importance, one is willing to make such assumptions in practice.

Classically, such assumptions are typically computational assumptions. We assume a particular problem such as factoring is difficult to solve, and in addition that the adversary has limited computational resources, in particular, not enough to solve the difficult problem. On the other hand, it is also possible to obtain security based on *physical* assumptions, where we first consider assuming that the adversary's memory resources are limited. Even a limit on classical memory can lead to security (Maurer, 1992; Cachin and Maurer, 1997). However, classical memory is typically cheap and plentiful. More significantly, however, Dziembowski and Maurer (2004) showed that any classical protocol in which the honest players need to store n bits to execute the protocol can be broken by an adversary who is able to store more than $O(n^2)$ bits. Motivated by this unsatisfactory gap it is an evident question to ask if quantum communication can be of any help. The situation is rather different if we allow quantum communication. We can have quantum protocols that require no quantum memory to be executed, but that are secure as long as the adversary's quantum memory is not larger than $n - O(\log^2 n)$ qubits (Dupuis, Fawzi, and Wehner, 2015), where n is the number of qubits sent during the protocol. This is essentially optimal, since any protocol that allows the adversary to store n qubits is known to be insecure (Lo, 1997; Lo and Chau, 1997; Mayers, 1997). The assumption of a memory limitation is known as the bounded (Damgaard *et al.*, 2008), or more generally, noisy-storage model (Wehner, Schaffner, and Terhal, 2008), as illustrated in Fig. 16.

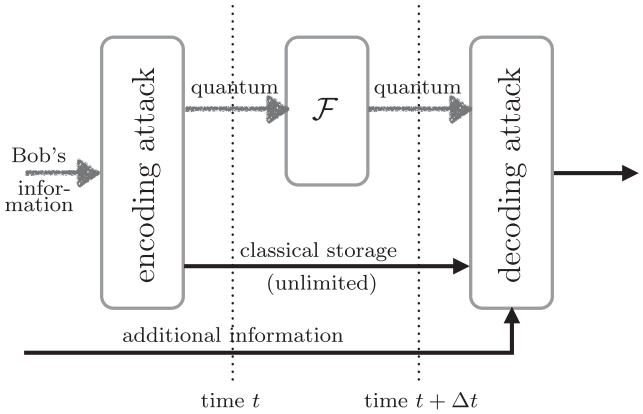


FIG. 16. The noisy-storage model: Wehner, Schaffner, and Terhal (2008) and König, Wehner, and Wullschleger (2012) assumed that during waiting times Δt in the protocol, the adversary can keep only quantum information in an imperfect and limited storage device described by a quantum channel $\mathcal{F}$. This is the only restriction and the adversary is otherwise arbitrarily powerful. In particular, he can first store all incoming qubits and has a quantum computer to encode them into an arbitrary quantum error-correcting code to protect them against the noise of the channel $\mathcal{F}$. He can also keep an unlimited amount of classical memory and perform any operation instantaneously.

Security proofs in this model are intimately connected to entropic uncertainty relations. Additionally, the uncertainty relations of Dupuis, Fawzi, and Wehner (2015) together with the work of König, Wehner, and Wullschleger (2012) demonstrated that any physical assumption that limits the adversary's entanglement leads to security.

1. Weak string erasure

The relation between cryptographic security and entropic uncertainty relations can easily be understood by looking at a simple cryptographic building block known as weak string erasure (WSE) (König, Wehner, and Wullschleger, 2012). Weak string erasure is universal for two-party secure computation in the sense that any other protocol can be obtained by repeated executions of weak string erasure, followed by additional quantum or classical communication (Kilian, 1988). Importantly, the storage assumption needs to hold only during some time Δt during the execution of weak string erasure.

Weak string erasure generates the following outputs if both Alice and Bob are honest: Alice obtains an n-bit string K^n, and Bob obtains a random subset $I \subseteq [n]$, and the bits $K_I \subseteq K^n$ as

indexed by the subset I. In addition, the following demands are made for security. If Bob is honest, then Alice does not know anything about I. In turn, if Alice is honest, then Bob should not know too much about K^n (except for K_I). More precisely, Bob should not be able to guess K^n too well, that is with Eq. (138),

$$H_{\min}(K^n|B) \geq \lambda \cdot n \text{ for some } \lambda \in [0,1], \tag{314}$$

where B denotes all of Bob's knowledge. See König, Wehner, and Wullschleger (2012) for a more detailed definition. A simple protocol for implementing weak string erasure is as follows.

(1) Alice prepares a random n-bit string K^n, encodes each bit K_i in one of the BB84 bases $\Theta \in \{\sigma_{\mathbb{X}}, \sigma_{\mathbb{Z}}\}$ at random, and sends these n qubits to Bob.
(2) Bob measures the n qubits in randomly chosen bases $\Theta' \in \{\sigma_{\mathbb{X}}, \sigma_{\mathbb{Z}}\}$.
(3) After the waiting time Δt, Alice sends the classical n-bit string Θ^n to Bob and outputs K^n.
(4) Bob computes $I = \{i : \theta_i = \theta_i'\}$ and outputs I and K_I.

Note that if both parties are honest, then the protocol is correct in the sense that Alice outputs K^n and Bob I with $K_I \subseteq K^n$. Moreover, when Alice is dishonest, it is intuitively obvious that she is unable to gain any information about the index set I (even with an arbitrary quantum memory), since she never receives any information from Bob during the protocol. A precise argument has been given by König, Wehner, and Wullschleger (2012). On the other hand, note that a dishonest Bob with a quantum memory can easily cheat by just keeping the n qubits he gets from Alice and wait until he receives the n-bit string Θ^n from Alice as well. Namely, he can then measure the n qubits in the same basis Θ^n as Alice and get the full n-bit string K^n [that is, $H_{\min}(K^n|B\Theta^n) = 0$]. However, if Bob has only a limited quantum memory, then he could not keep a perfect copy of the n qubits he gets from Alice.

The security analysis is linked immediately to a guessing game whenever we consider a purified version of the protocol in which Alice does not prepare BB84 states herself, but instead makes EPR pairs $|\psi\rangle_{AB} = (|00\rangle_{AB} + |11\rangle_{AB})/\sqrt{2}$ and sends B to Bob, while measuring A in a randomly chosen BB84 basis. In the analysis, one can indeed give even more power to Bob by letting him prepare a state ρ_{AB} in each round of the protocol and Alice measures A in a randomly chosen BB84 basis. Alice then sends him the basis choice. Recall that $H_{\min}(K^n|B\Theta^n) = -\log p_{\text{guess}}(K^n|B\Theta^n)$, that is, the min-entropy security guarantee that WSE demands are precisely related to Bob's ability to win the guessing game (Ballester, Wehner, and Winter, 2008). The storage assumption translates into one particular example of how the entanglement in ρ_{AB} is limited, putting a limit on $H_{\min}(A|B)$ of the states that Bob can prepare.

2. Bounded-storage model

To illustrate further how a bound on entropic uncertainty leads to security, let us first consider a special case of the noisy-storage model, also known as the bounded-storage model. Here the channel $\mathcal{F} = \mathcal{I}_2^{\otimes q}$ in Fig. 16 is just the identity on q qubits. This bounded-storage model was introduced and first studied by Damgaard *et al.* (2007, 2008) and Schaffner (2007).

While more refined bounds are known (Dupuis, Fawzi, and Wehner, 2015), let us first explain how entropic uncertainty relations for a classical memory system can be used to obtain weak security statements in this setting. To this end, we differentiate Bob's knowledge into $B = QM\Theta^n$, where Q denotes the q qubits of quantum memory, M denotes (unbounded) classical information, and Θ^n is the n-bit basis information string Alice sent to Bob. Since the conditional min-entropy obeys a chain rule (Renner, 2005), we can separate the quantum memory as

$$H_{\min}(K^n|B) = H_{\min}(K^n|QM\Theta^n) \tag{315}$$

$$\geq H_{\min}(K^n|M\Theta^n) - q. \tag{316}$$

Analyzing $H_{\min}(K^n|M\Theta^n)$ is then directly determined by Bob's ability to win the guessing game, in which he has only classical information M. Using the min-entropy uncertainty relation (102) for the n qubit BB84 measurements (with an extension to classical side information M as sketched in Sec. IV.C), we get

$$H_{\min}(K^n|M\Theta^n) \geq -n \cdot \log\left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right). \tag{317}$$

Hence, we find a nontrivial lower bound

$$H_{\min}(K^n|B) > 0 \tag{318}$$

as long as $q \lesssim n \cdot 0.22$. This security analysis can be refined and improving on the work of Damgaard *et al.* (2007), Ng, Berta, and Wehner (2012) made use of the following stronger smooth min-entropy uncertainty relation which is based on Eq. (103):

$$H_{\min}^{\varepsilon}(K^n|M\Theta^n) \geq n \cdot \sup_{s\in(0,1]}\left(\frac{1}{s}[1 + s - \log(1+2^s)] - \frac{1}{sn}\log\frac{2}{\varepsilon^2}\right). \tag{319}$$

One can use this uncertainty relation together with the more refined analysis of König, Wehner, and Wullschleger (2012) instead of Eq. (316), to obtain perfect security ($\lambda \to 1$) against quantum memory of size

$$q \leq \frac{n}{2} \tag{320}$$

for $n \to \infty$. Ultimately, Dupuis, Fawzi, and Wehner (2015) showed by deriving strong entropic uncertainty relations that the protocol from Sec. VI.C.1 implements a WSE scheme against q qubits of quantum memory for

$$\lambda = \frac{1}{2}\left[\gamma_{BB84}\left(-\frac{q}{n}\right) - \frac{1}{n}\right], \tag{321}$$

where the function $\gamma_{BB84}(\cdot)$ is as in Eq. (202). Asymptotically ($n \to \infty$), this provides perfect security ($\lambda \to 1$) against quantum memories of size

$$q \leq n - O(\log^2 n). \tag{322}$$

This is basically optimal, since no protocol can be secure if $q = n$. Finally, we mention that alternatively we could also use a six-state encoding $\{\sigma_{\mathbb{X}}, \sigma_{\mathbb{Y}}, \sigma_{\mathbb{Z}}\}$ for the weak string erasure protocol described in Sec. VI.C.1. See Mandayam and Wehner (2011), Ng, Berta, and Wehner (2012), and Dupuis, Fawzi, and Wehner (2015) for a security analysis.

3. Noisy-storage model

Let us now consider the general case of arbitrary storage devices $\mathcal{F}$ in Fig. 16 (Wehner, Schaffner, and Terhal, 2008). This model is motivated by the fact that counting qubits is generally a significant overestimate of the storage capabilities of a quantum memory, and indeed, for example, for continuous variable systems there is no dimension bound to which to apply the bounded-storage analysis. The first general security analysis was given by König, Wehner, and Wullschleger (2012), which was then refined significantly by Berta *et al.* (2013) and Berta, Fawzi, and Wehner (2014), leading to the asymptotically tight security analysis by Dupuis, Fawzi, and Wehner (2015). Here one cannot just use the chain rule to separate the quantum memory as in Eqs. (315) and (316). Such a separation is possible only when relating the security to the classical capacity of the storage channel $\mathcal{F}$ (König, Wehner, and Wullschleger, 2012). Instead, we have to apply a min-entropy uncertainty relation with quantum memory to directly lower bound

$$H_{\min}(K^n|B) = H_{\min}(K^n|QM\Theta^n). \tag{323}$$

We use a variant of Eq. (201) for the n qubit BB84 measurements to bound (Dupuis, Fawzi, and Wehner, 2015)

$$H^{\varepsilon}_{\min}(K^n|QM\Theta^n) \geq n \cdot \gamma_{\mathrm{BB84}}\left(\frac{H_{\min}(A^n|QM)}{n}\right) - 1 - \log\left(\frac{2}{\varepsilon^2}\right), \tag{324}$$

where the function $\gamma_{\mathrm{BB84}}(\cdot)$ is as in Eq. (202). In order to get an idea how to lower bound the right-hand side of Eq. (324) under a noisy quantum memory Q assumption, recall that $H_{\min}(A^n|QM)$ is a measure of entanglement between A^n and $B = QM$. In particular, one can relate this amount of entanglement to Bob's ability to store the n EPR pairs that Alice sends in the purified version of the protocol, that is, the quantum capacity of the storage channel $\mathcal{F}$. If $\mathcal{F}$ cannot preserve said entanglement, then $H_{\min}(K^n|QM\Theta^n)$ in Eq. (324) will be lower bounded nontrivially leading to a secure WSE scheme for some trade-off between the security parameter λ from Eq. (314), the number n of qubits sent, and the noisiness of the quantum memory Q. See Dupuis, Fawzi, and Wehner (2015) for details.

Again we could also use a six-state encoding $\{\sigma_{\mathbb{X}}, \sigma_{\mathbb{Y}}, \sigma_{\mathbb{Z}}\}$ for the weak string erasure protocol described in Sec. VI.C.1. See Berta, Fawzi, and Wehner (2014) and Dupuis, Fawzi, and Wehner (2015) for a security analysis.

4. Uncertainty in other protocols

Many other quantum cryptographic protocols were analyzed via entropic uncertainty relations (Broadbent and Schaffner, 2016). The entropic relation for channels (241) was used by Buhrman *et al.* (2008) to obtain cheat sensitivity for a quantum string commitment protocol. The same relations as relevant for the noisy-storage model have also been used to prove security in the isolated qubit model (Liu, 2014, 2015). In this model, the adversary is given a quantum memory of potentially long-lived qubits, but they are isolated in the sense that he is unable to perform coherent operations on many qubits simultaneously. In particular, the uncertainty relation of Damgaard *et al.* (2007) was used by Liu (2014) to obtain security. It is possible to use Eq. (103) from Ng, Berta, and Wehner (2012) to obtain improved security parameters. Furthermore, tripartite (Tomamichel *et al.*, 2013) uncertainty relations have been used to ensure the security of position-based cryptography. Finally, in relativistic cryptography, security of two-party protocols is possible under the assumptions that each player is split into several noncommunicating agents. Tripartite uncertainty relations have been used to establish security in this setting (Kaniewski *et al.*, 2013).

D. Entanglement witnessing

Entanglement is a central resource in quantum information processing. Hence, methods for detecting entanglement are crucial for quantum information technologies. Entanglement witnessing refers to the process of verifying that a source is producing entangled particles. Entangled states are defined as those states that are nonseparable, i.e., they cannot be written as a convex combination of product states. A common theme in entanglement witnessing is to prove a mathematical identity that all separable states must satisfy; let us refer to such an identity as an entanglement witness. Experimentally demonstrating that one's source violates this identity will then guarantee that the source produces entangled particles.

Entanglement witnessing is a well-developed field [see, e.g., the review articles by Gühne and Tóth (2009) and Horodecki *et al.* (2009)], and there are many types of entanglement witnesses. Here we focus mostly on entanglement witnesses that follow from entropic uncertainty relations.

In what follows, we restrict the discussion to bipartite entanglement. We note that entanglement witnessing typically occurs in the distant-laboratories paradigm, where two parties (Alice and Bob) can each perform local measurements on their respective systems, but neither party can perform a global measurement on the bipartite system.

For introductory purposes, let us mention a simple, well-known bipartite entanglement witness for two qubits. Although it is nonentropic, it is based on complementary observables, and so it can be directly compared to the entropic witnesses discussed below. Namely, consider the operator

$$E_{XZ} := E_X + E_Z, \tag{325}$$

where

$$E_X := |+\rangle\langle+| \otimes |-\rangle\langle-| + |-\rangle\langle-| \otimes |+\rangle\langle+|, \tag{326}$$

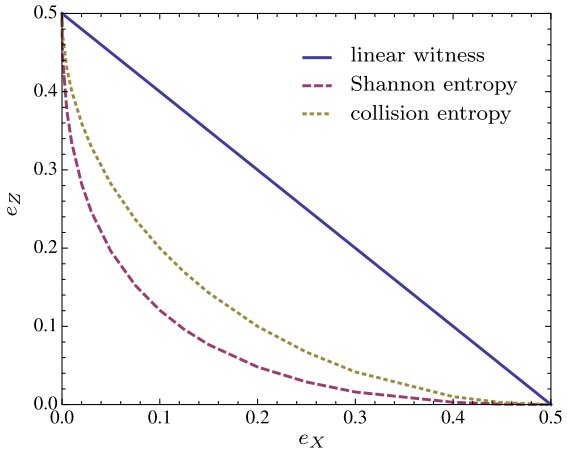


FIG. 17. Entanglement witnessing for a bipartite two-qubit state using mutually unbiased observables. Suppose Alice and Bob observe $\Pr[X_A=X_B=0]=\Pr[X_A=X_B=1]=(1-e_X)/2$ and $\Pr[X_A=0,X_B=1]=\Pr[X_A=1,X_B=0]=e_X/2$, and analogously for Z and e_Z. The region below the curve indicates the region for which one can guarantee entanglement for the respective witnesses.

$$E_Z \coloneqq |0\rangle\langle 0| \otimes |1\rangle\langle 1| + |1\rangle\langle 1| \otimes |0\rangle\langle 0|. \tag{327}$$

Note that E_X and E_Z are "error operators" in that they project onto the subspaces where Alice's and Bob's measurement outcomes are different. For a maximally entangled state of the form $|\psi\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$, there is no probability for error in either basis, so we have $\langle\psi|E_{XZ}|\psi\rangle = 0$. On the other hand, for any separable state ρ_{AB}, we have that [see, e.g., Namiki and Tokunaga (2012)]

$$\mathrm{tr}[\rho_{AB}E_{XZ}] \geq \tfrac{1}{2}. \tag{328}$$

Hence, if $\langle E_X\rangle + \langle E_Z\rangle < 1/2$, where $\langle O\rangle \coloneqq \mathrm{tr}[O\rho_{AB}]$, then ρ_{AB} is entangled. This witness is depicted as the solid line in Fig. 17.

1. Shannon entropic witness

Some early work on entanglement witnessing using entropic uncertainty relations was done by Giovannetti (2004) and Gühne and Lewenstein (2004), and further improvements were later made by Huang (2010). The following discussion focuses primarily on more recent developments, e.g., where entanglement witnessing is based on the bipartite uncertainty relation with quantum memory in Eq. (165). Berta *et al.* (2010) discussed how this can be used for entanglement witnessing, and the approach was implemented by Li *et al.* (2011) and Prevedel *et al.* (2011). Specifically, from Eq. (165), one finds that all separable states satisfy

$$H(X_A|X_B) + H(Z_A|Z_B) \geq q_{\mathrm{MU}}, \tag{329}$$

where the q_{MU} parameter refers to Alice's observables, and Bob's observables $\mathbb{X}_B$ and $\mathbb{Z}_B$ are arbitrary. One can see this by noting that $H(A|B) \geq 0$ for any separable state, and furthermore that measuring Bob's system in some basis $\mathbb{X}_B$ cannot reduce his uncertainty about Alice's measurement, i.e., $H(X_A|X_B) \geq H(X_A|B)$.

One can use Eq. (329) for entanglement witnessing, using a protocol where Alice and Bob have many copies of ρ_{AB} and they both measure on each copy either their $\mathbb{X}$ or $\mathbb{Z}$ observable. The quantities $H(X_A|X_B)$ and $H(Z_A|Z_B)$ can then be calculated from their joint probability distributions $\Pr(X_A = x_A, X_B = x_B)$ and $\Pr(Z_A = z_A, Z_B = z_B)$, and if Eq. (329) is violated, then ρ_{AB} must be entangled.

Figure 17 depicts this entanglement witness (long-dashed curve) for the case of qubits and mutually unbiased bases. A comparison of this curve to the black line shows that Eq. (328) detects more entangled states than Eq. (329). However, the "quality" of entanglement that Eq. (329) detects is higher. This is because Eq. (329) holds for all nondistillable states, i.e., states from which Alice and Bob cannot distill any EPR (maximally entangled) states using local operations and classical communication [see, e.g., Horodecki *et al.* (2009) for a discussion of local operations and classical communication]. In this sense, Eq. (329) detects *distillable* entanglement whereas Eq. (328) detects all forms of entanglement.

One can make this quantitative using a result by Devetak and Winter (2005) that the coherent information (i.e., minus the conditional entropy) lower bounds the distillable entanglement E_D, i.e., the optimal asymptotic rate for distilling EPR states using local operation and classical communication:

$$E_D \geq -H(A|B). \tag{330}$$

Combining this with Eq. (165) gives

$$E_D \geq q_{\mathrm{MU}} - H(X_A|X_B) - H(Z_A|Z_B). \tag{331}$$

This reveals an advantage of the entropic uncertainty approach to entanglement witnessing. Namely, that it can give quantitative lower bounds, in contrast to witnesses like that in Eq. (328) that answer only a "yes or no" question.

Another advantage of the entropic uncertainty approach is that it requires no structure on Bob's side. While Eq. (328) requires both Alice's and Bob's measurements to be mutually unbiased, the entropic uncertainty approach allows for arbitrary measurements on Bob's system.

2. Other entropic witnesses

Bipartite quantum memory uncertainty relations generally lead to entanglement witnesses. For example, Berta, Coles, and Wehner (2014) discussed how the uncertainty relation in Eq. (185) allows for entanglement witnessing using a set of n MUBs on Alice's system (more precisely, a subset of size n of MUBs chosen from a set of $d_A + 1$ MUBs, where d_A is a prime power and $2 \leq n \leq d_A + 1$). Consider such a set $\{\mathbb{X}_j\}$ of n MUBs on Alice's system, and consider a set of n arbitrary POVMs $\{\mathbb{Y}_j\}$ on Bob's system. Berta, Coles, and Wehner (2014) showed that all separable states must satisfy

$$\sum_{j=1}^{n} 2^{-H_2(X_j|Y_j)} \leq 1 + \frac{n-1}{d_A}. \tag{332}$$

Figure 17 compares this entanglement witness (short-dashed curve) to the previously discussed ones, in the qubit case with $n = 2$. Note that Eq. (332) detects more entangled states than Eq. (329), but not as much as Eq. (328).

Similar to the Shannon entropy case in Eq. (331), the uncertainty relation (185) actually allows one to give a quantitative lower bound on an entanglementlike measure. Namely, Eq. (185) allows one to lower bound $-H_{\mathrm{coll}}(A|B)$.

3. Continuous variable witnesses

The method of witnessing entanglement through entropic uncertainty relations was also extended to continuous variable systems by Walborn *et al.* (2009), and further studied by Saboia, Toscano, and Walborn (2011) and Huang (2013).

E. Steering inequalities

First highlighted by Schrödinger (1935), steering is a phenomenon for bipartite quantum systems that is related to entanglement (although not precisely the same). As in the previous section, we consider the distant-laboratories paradigm involving two parties, Alice and Bob, where Alice (Bob) has access to system A (B). Steering corresponds to one party's (say Alice's) measurement choice giving rise to different ensembles of states on the other party's (Bob's) system. Not all quantum states exhibit steering, e.g., separable states are nonsteerable. At the other extreme, all states that violate a Bell inequality are steerable. While Bell inequalities are derived for states that admit a local hidden variable model, Wiseman, Jones, and Doherty (2007) formalized the notion of steerability as those states ρ_{AB} that do not admit a local hidden state (LHS) model. An LHS model is a model where, say, system B has a local quantum state that is classically correlated to arbitrary observables on system A. This formalization has led researchers to derive steering inequalities (Cavalcanti *et al.*, 2009), in analogy to Bell inequalities.

Walborn *et al.* (2011) and Schneeloch *et al.* (2013) showed how entropic uncertainty relations can be used to derive steering inequalities. The idea is that if B has a local hidden state, then its measurement probabilities must obey a single system uncertainty relation, even if they are conditioned on the measurement outcomes on A. More precisely, an LHS model implies that the joint probability distribution for discrete observables $\mathbb{X}_A$ on A and $\mathbb{X}_B$ on B has the form

$$P(\mathbb{X}_A, \mathbb{X}_B) = \sum_\lambda P(\Lambda = \lambda) P(\mathbb{X}_A|\Lambda = \lambda) P_Q(\mathbb{X}_B|\Lambda = \lambda). \tag{333}$$

Here Λ is the hidden variable that determines Bob's local state, λ is a particular value that this variable may take, and the subscript Q on $P_Q(\mathbb{X}_B|\Lambda = \lambda)$ emphasizes that the probability distribution arises from a single quantum state. Next we have

$$H(X_B|X_A) \geq H(X_B|X_A\Lambda) \tag{334}$$

$$= \sum_\lambda P(\Lambda = \lambda) H(X_B|X_A\Lambda = \lambda) \tag{335}$$

$$= \sum_\lambda P(\Lambda = \lambda) H(X_B|\Lambda = \lambda), \tag{336}$$

where the notation $H(X_B|X_A\Lambda = \lambda)$ should be read as the entropy of X_B conditioned on X_A and conditioned on the event that $\Lambda = \lambda$. Hence, for two observables $\mathbb{X}_B$ and $\mathbb{Z}_B$ on B, and some other observables $\mathbb{X}_A$ and $\mathbb{Z}_A$ on A, we have

$$H(X_B|X_A) + H(Z_B|Z_A) \geq \sum_\lambda P(\Lambda = \lambda)[H(X_B|\Lambda = \lambda) + H(Z_B|\Lambda = \lambda)]. \tag{337}$$

Combining this with, say, Maassen-Uffink's uncertainty relation (31) gives the following steering inequality (Schneeloch *et al.*, 2013):

$$H(X_B|X_A) + H(Z_B|Z_A) \geq q_{\mathrm{MU}}, \tag{338}$$

where q_{MU} refers to Bob's observables. Any state ρ_{AB} that admits an LHS model must satisfy Eq. (338). Hence, an experimental violation of Eq. (338) would constitute a demonstration of steering. Similar steering inequalities can be derived for continuous variables (Walborn *et al.*, 2011).

F. Wave-particle duality

Wave-particle duality is the fundamental concept that a single quantum system can exhibit either wave behavior or particle behavior: one cannot design an interferometer that can simultaneously show both behaviors. This idea was qualitatively discussed by Feynman and was subsequently put on quantitative grounds by Wootters and Zurek (1979), Jaeger, Shimony, and Vaidman (1995), Englert (1996), and Englert and Bergou (2000), and others, who proved inequalities known as wave-particle duality relations (WPDRs). Many such relations consider the Mach-Zehnder interferometer for single photons, shown in Fig. 18. In this case, particle behavior is associated with knowing the path that the photon travels through the interferometer. Wave behavior, on the other hand, is associated with seeing oscillations in the probability to detect the photon in a given output mode as one varies the relative phase ϕ between the two interferometer arms. Denoting the which-path observable as $\mathbb{Z} = \{|0\rangle\langle 0|, |1\rangle\langle 1|\}$, particle behavior can be quantified by the path predictability $\mathcal{P} = 2p_{\mathrm{guess}}(Z) - 1$ [which is related to the probability $p_{\mathrm{guess}}(Z)$ of guessing the path correctly]. The wave behavior is quantified by the fringe visibility

$$\mathcal{V} = \frac{p_0^{\max} - p_0^{\min}}{p_0^{\max} + p_0^{\min}} \quad \text{with} \quad p_0^{\max} := \max_\phi p_0, \quad p_0^{\min} := \min_\phi p_0, \tag{339}$$

where p_0 is the probability for the photon to be detected by D_0 (see Fig. 18). Wootters and Zurek (1979) proved that

$$\mathcal{P}^2 + \mathcal{V}^2 \leq 1, \tag{340}$$

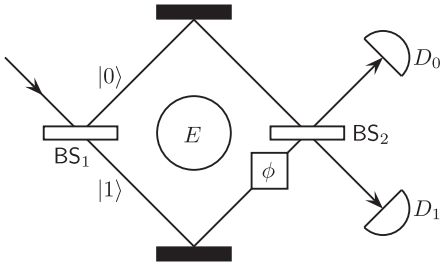


FIG. 18. Mach-Zehnder interferometer for single photons. A photon impinges on a beam splitter, after which we label the two possible paths by the $\mathbb{Z}$ basis states $|0\rangle, |1\rangle$. The photon may interact with some environment E inside the interferometer. Then a phase ϕ is applied to the lower path, and the two paths are recombined on a second beam splitter. Finally the photon is detected at either D_0 or D_1.

which implies $\mathcal{V} = 0$ when $\mathcal{P} = 1$ (full particle behavior means no wave behavior) and vice versa.

More generally, suppose the photon interacts with some environment system E inside the interferometer. Measuring E might reveal, e.g., some information about which path the photon took, so it is natural to consider the path distinguishability

$$\mathcal{D} = 2p_{\text{guess}}(Z|E) - 1. \tag{341}$$

Jaeger, Shimony, and Vaidman (1995) and Englert (1996) proved a stronger version of Eq. (340), namely,

$$\mathcal{D}^2 + \mathcal{V}^2 \leq 1. \tag{342}$$

WPDRs such as Eqs. (340) and (342) have often been thought to be conceptually different from uncertainty relations, although this has been debated. For example, Dürr and Rempe (2000) and Busch and Shilladay (2006) found connections between certain WPDRs and Robertson's uncertainty relation involving the standard deviation. More recently, Coles, Kaniewski, and Wehner (2014) showed that Eqs. (340), (342), and some other WPDRs are actually entropic uncertainty relations in disguise. In particular, they correspond to the uncertainty relation for the min- and max-entropies in Eq. (222), applied to complementary qubit observables. Namely, Eq. (340) is equivalent to the uncertainty relation,

$$H_{\min}(Z) + \min_{W \in XY} H_{\max}(W) \geq 1, \tag{343}$$

where the $\min_{W \in XY}$ corresponds to minimizing over all observables in the x-y plane of the Bloch sphere. Likewise Eq. (342) is equivalent to the uncertainty relation

$$H_{\min}(Z|E) + \min_{W \in XY} H_{\max}(W) \geq 1. \tag{344}$$

This unifies the wave-particle duality principle with the entropic uncertainty principle, showing that the former is a special case of the latter.

Naturally, other entropies could be used in place of the min- and max-entropies, and although one might not obtain a precise equivalence to the WPDRs, the conceptual meaning may be similar. Bosyk *et al.* (2013) took this approach using uncertainty relations involving Rényi entropies. Vaccaro (2011) employed the Shannon entropy to formulate a WPDR in terms of the mutual information. Moreover, they added the conceptual insight that wave and particle behavior are related to symmetry and asymmetry, respectively. Finally, Englert *et al.* (2008) considered entropic measures of wave and particle behavior for interferometers with more than two paths.

G. Quantum metrology

Quantum metrology deals with the physical limits on the accuracy of measurements (Giovannetti, Lloyd, and Maccone, 2011). The uncertainty principle plays an important role in establishing such physical limits. Typically in quantum metrology one is interested in estimating an optical phase, e.g., the phase shift in an interferometer (as in Fig. 18). Hence, uncertainty relations involving the phase have applications here. Recall that we briefly discussed an entropic uncertainty relation for the number and phase in Sec. V.F, specifically in Eq. (299). While quantum metrology is a broad field [see, e.g., Giovannetti, Lloyd, and Maccone (2011) for a review], we mention here a few works that exploit entropic uncertainty relations.

The Heisenberg limit is a well-known limit in quantum metrology stating that the uncertainty in the phase estimation scales as $1/\langle N \rangle$. Here $\langle N \rangle$ is the mean photon number of the light that is used to probe the phase. Hall *et al.* (2012) noted that the Heisenberg limit is heuristic and put it on rigorous footing by proving the following bound:

$$\delta\hat{\Phi} \geq k/\langle N + 1 \rangle, \tag{345}$$

where $\delta\hat{\Phi}$ is the root-mean-square deviation of the phase estimate $\hat{\Phi}$ from the actual phase Φ, and $k \coloneqq \sqrt{2\pi/e^2}$. To prove Eq. (345), Hall *et al.* (2012) defined the random variable $\Theta \coloneqq \hat{\Phi} - \Phi$ and applied the entropic uncertainty relation in Eq. (299), giving

$$H(N) + h(\Theta) \geq \log 2\pi. \tag{346}$$

Then they combined Eq. (346) with some identities that relate $h(\Theta)$ to $\delta\hat{\Phi}$ and $H(N)$ to $\langle N + 1 \rangle$.

Hall and Wiseman (2012) considered a more general scenario where one may have some prior information about the phase, and they likewise used the entropic uncertainty relation in Eq. (299) to obtain a rigorous statement of the Heisenberg limit.

H. Other applications in quantum information theory

Recent efforts to understand the classical-quantum boundary, in the context of both physics and information processing, have led to quantitative measures of "quantumness" like coherence and discord, which are discussed in Secs. VI.H.1 and VI.H.2, respectively. We further discuss information

locking in Sec. VI.H.3 and touch on quantum coding in Sec. VI.H.4.

1. Coherence

Baumgratz, Cramer, and Plenio (2014) introduced a framework for quantifying coherence, which is a measure that does not increase under incoherent operations. There are a variety of coherence measures, but one, in particular, has an operational meaning in terms of the number of distillable maximally coherent states (Winter and Yang, 2016),

$$\Phi(\mathbb{Z},\rho) \coloneqq D\left(\rho\|\sum_z |\mathbb{Z}^z\rangle\langle\mathbb{Z}^z|\rho|\mathbb{Z}^z\rangle\langle\mathbb{Z}^z|\right), \tag{347}$$

the relative entropy of coherence. Note that the coherence is a function of the state ρ as well as an orthonormal basis $\mathbb{Z} = \{|\mathbb{Z}^z\rangle\langle\mathbb{Z}^z|\}$.

The following connection between coherence and entropic uncertainty was established by Coles *et al.* (2011, 2012b). Let ρ_S be any state for system S and let $\mathbb{Z}$ be a projective measurement on S. Then, we have

$$\Phi(\mathbb{Z},\rho_S) = H(Z|E), \tag{348}$$

where E is a purifying system for ρ_S. This states that the relative entropy of coherence for a projective measurement is equivalent to the uncertainty of that measurement given the purifying system, or in other words, given access to the environment E. The right-hand side of Eq. (348) quantifies uncertainty in the presence of quantum memory, and uncertainty relations for such measures have been discussed in Sec. IV. Hence, one can reinterpret such uncertainty relations as, e.g., in Eq. (165), as lower bounds on the *coherence* of ρ_S for different measurements. This idea was discussed by Korzekwa *et al.* (2014), although they focused more on the perspective of Luo (2005) of separating total uncertainty into "classical" and "quantum" parts. In particular, for a rank-one projective measurement $\mathbb{Z} = \{|\mathbb{Z}^z\rangle\langle\mathbb{Z}^z|\}$ and a quantum state ρ, they defined the classical uncertainty as the entropy of the state $C(\mathbb{Z},\rho) \coloneqq H(\rho)$, and the quantum uncertainty as the relative entropy of coherence,

$$Q(\mathbb{Z},\rho) \coloneqq D\left(\rho\|\sum_z |\mathbb{Z}^z\rangle\langle\mathbb{Z}^z|\rho|\mathbb{Z}^z\rangle\langle\mathbb{Z}^z|\right). \tag{349}$$

It is straightforward to show that overall uncertainty is the sum of the classical and quantum parts

$$H(Z) = Q(\mathbb{Z},\rho) + C(\mathbb{Z},\rho). \tag{350}$$

Korzekwa *et al.* (2014) derived several uncertainty relations for the quantum uncertainty $Q(\mathbb{Z},\rho)$. However, using Eq. (348), one can reinterpret their relations as entropic uncertainty relations in the presence of quantum memory. In particular, their uncertainty relations follow directly from combining Eq. (165) with Eq. (348).

2. Discord

Ollivier and Zurek (2001) quantified quantum correlations by discord,

$$D(B|A) \coloneqq I(A:B) - J(B|A), \tag{351}$$

which is the difference between the quantum mutual information $I(A:B)$ and the classical correlations,

$$J(B|A) \coloneqq \max_{\mathbb{X}} I(X:B), \tag{352}$$

where the optimization is over all POVMs $\mathbb{X}$ acting on system A. In Sec. IV.E, example 26, we discussed how discord quantifies the gap between conditioning on classical versus quantum memory. Another connection to discord is the following. In an effort to strengthen the uncertainty relation with quantum memory in Eq. (165), Pati *et al.* (2012) introduced an additional term that depends on the discord of the state ρ_{AB}. Namely, they proved the inequality

$$H(X|B) + H(Z|B) \geq q_{\mathrm{MU}} + H(A|B) + \max\{0, D(B|A) - J(B|A)\}. \tag{353}$$

Clearly this strengthens the bound in Eq. (165) for states ρ_{AB} whose discord exceeds their classical correlations $D(B|A) > J(B|A)$. Indeed, Pati *et al.* (2012) showed that this is true for Werner states, for which Eq. (353) becomes an equality.

In turn, this result was used by Hu and Fan (2013b) to obtain a strong upper bound on discord. That is, the uncertainty relation (353) allows one to bound the discord by

$$D(B|A) \leq \tfrac{1}{2}[I(A:B) + \delta_T], \tag{354}$$

where

$$\delta_T \coloneqq H(X|B) + H(Z|B) - q_{\mathrm{MU}} - H(A|B). \tag{355}$$

Here δ_T is the gap between the left- and right-hand sides in the uncertainty relation (165).

Further connections between quantum correlations and entropic uncertainty relations have been elucidated in the context of non-Markovian dynamics (Karpat, Piilo, and Maniscalco, 2015), entanglement creation (Coles, 2012a), teleportation (Hu and Fan, 2012), and monogamy (Hu and Fan, 2013a).

3. Locking of classical correlations

One operational way of understanding entropic uncertainty relations is in terms of information locking (DiVincenzo *et al.*, 2004). In the following we present a cryptographic view on information locking as discussed by Fawzi, Hayden, and Sen (2011).

A locking scheme is a protocol that encodes a classical message into a quantum state using a classical key of size smaller than the message. The goal is that without knowing the key the message is locked in the quantum state such that any possible measurement reveals only a negligible amount of information about the message. Furthermore, knowing the key

it is possible to unlock and completely recover the message. The connection of information locking to entropic uncertainty is best presented by means of a simple example based on the Maassen-Uffink bound for the n qubit BB84 measurements (101),

$$H(K^n|\Theta^n) \geq n \cdot \tfrac{1}{2}, \tag{356}$$

with $\Theta^n \in \{\theta_1, \ldots, \theta_{2^n}\}$. In order to encode a uniformly random n-bit string X we choose at random an n qubit BB84 basis θ_i (the key) and encode the message in this basis. Based on Eq. (356), DiVincenzo *et al.* (2004) showed that for any measurement on this quantum state the mutual information (accessible information) between the outcome of that measurement and the original classical message X is at most $n/2$. That is, $n/2$ bits are locked in the quantum state and are not accessible without knowing the basis choice (the key). This is remarkable because any nontrivial purely classical encryption of an n-bit string message requires a key of size at least n. Of course, this then raises the question about the optimal trade-off between the number of lockable bits and the key size. For that purpose Fawzi, Hayden, and Sen (2011) made use of the uncertainty relation (100),

$$H(K|\Theta) \geq n \cdot (1 - 2\varepsilon) - h_{\text{bin}}(\varepsilon), \tag{357}$$

with $\Theta = \{\theta_1, \ldots, \theta_L\}$. Based on this they showed that a key size of $L = O\big(\log(n/\varepsilon)\big)$ allows for locking an n-bit string up to a mutual information smaller than $\varepsilon > 0$. State-of-the-art results use stronger definitions for information locking in terms of the trace norm instead of the mutual information and are based on so-called metric uncertainty relations (Fawzi, Hayden, and Sen, 2011; Dupuis *et al.*, 2013).[35] Finally, we mention that Guha *et al.* (2014) initiated the study of the information locking capacity of quantum channels, which is also intimately related to uncertainty.

4. Quantum Shannon theory

The original partial results and conjectures for entropic uncertainty relations with quantum memory by Christandl and Winter (2005) and Renes and Boileau (2008, 2009) were inspired by applications in quantum Shannon theory. More recently, entropic uncertainty relations and, in particular, their equality conditions have been used to analyze the performance of quantum polar codes (Renes and Wilde, 2014; Renes *et al.*, 2015).

VII. MISCELLANEOUS TOPICS

A. Tsallis and other entropy functions

From a mathematical perspective it is insightful to consider uncertainty relations for various generalizations of the Shannon entropy. While the Rényi entropies were discussed previously, the Tsallis entropies are another family of interest. The Tsallis entropy of order α is defined as

$$H_\alpha^T(X) := \left(\frac{\log e}{1-\alpha}\right)\left(\sum_x P_X(x)^\alpha - 1\right) \tag{358}$$

for $\alpha \in (0,1)\cup(1,\infty)$, and as the corresponding limit for $\alpha \in \{0, 1, \infty\}$. Similar to the Rényi entropies, the $\alpha = 1$ Tsallis entropy corresponds to the Shannon entropy. Note that for $x \approx 1$ we have $\log x \approx \log e \cdot (x-1)$, so when $\sum_x P_X(x)^\alpha \approx 1$ the Tsallis entropy approximates the Rényi entropy.

Rastegin studied uncertainty relations in terms of the Tsallis entropy. For example, Rastegin (2013a) proved the following uncertainty relation for Tsallis entropies for a set of three MUBs $\{\mathbb{X}, \mathbb{Y}, \mathbb{Z}\}$ on a qubit. For $\alpha \in (0,1]$ and for integers $\alpha \geq 2$, we have

$$H_\alpha^T(X) + H_\alpha^T(Y) + H_\alpha^T(Z) \geq 2\log e \cdot f_\alpha(2), \tag{359}$$

where

$$f_\alpha(x) := \left(\frac{1 - x^{1-\alpha}}{\alpha - 1}\right). \tag{360}$$

This generalizes the result in Eq. (79), which is recovered by taking the limit $\alpha \to 1$, noting that $\lim_{\alpha\to 1} f_\alpha(x) = \log x / \log e$.

A more general scenario was considered by Rastegin (2013b), where system A has dimension d, and the measurements under consideration form a set of n MUBs, $\{\mathbb{X}_j\}$. For $\alpha \in (0,2]$, Rastegin (2013b) showed that

$$\frac{1}{n}\sum_{j=1}^n H_\alpha^T(X_j) \geq 2\log e \cdot f_\alpha\left(\frac{nd}{n+d-1}\right). \tag{361}$$

This result is quite general in that it holds for any n and d. Furthermore, in the case of $n = d+1$ and $\alpha \to 1$, one recovers the result presented in Eq. (81). Rastegin (2013b) also tightened Eq. (361) for mixed states:

$$\frac{1}{n}\sum_{j=1}^n H_\alpha^T(X_j) \geq 2\log e \cdot f_\alpha\left(\frac{nd}{n + d\,\mathrm{tr}(\rho^2) - 1}\right). \tag{362}$$

Other entropy families are also discussed in the literature. For example, Zozor, Bosyk, and Portesi (2014) considered a broad class of entropies defined as

$$H_{(\eta,\phi)}(X) := \eta\left(\sum_x \phi(P_X(x))\right). \tag{363}$$

Here $\eta\colon \mathbb{R} \to \mathbb{R}$ and $\phi\colon [0;1] \to \mathbb{R}$ are generic continuous functions such that either ϕ is strictly concave and η is strictly increasing, or ϕ is strictly convex and η is strictly decreasing. Additionally, they imposed $\phi(0) = 0$ and $\eta(\phi(1)) = 0$. This family includes as special cases both the Rényi and Tsallis families and hence also the Shannon entropy. In addition to

[35] We emphasized that the security definitions for information locking are not composable [see, e.g., Renner (2005) for a discussion].

giving an overview of the literature on entropic uncertainty relations, Zozor, Bosyk, and Portesi (2014) derived a new uncertainty relation for the $H_{(\eta,\phi)}$ entropies. For any two POVMs $\mathbb{X}$ and $\mathbb{Z}$, and for any two pairs of functionals (η_1,ϕ_1) and (η_2,ϕ_2), their relation takes the form

$$H_{(\eta_1,\phi_1)}(X)+H_{(\eta_2,\phi_2)}(Z)\geq B_{(\eta_1,\phi_1),(\eta_2,\phi_2)}(t), \quad (364)$$

where the right-hand side is a function of the triplet

$$t\coloneqq\{c_{\mathbb{X}},c_{\mathbb{Z}},c\},\qquad c_{\mathbb{X}}\coloneqq\max_x\|\mathbb{X}^x\|,\qquad c_{\mathbb{Z}}\coloneqq\max_z\|\mathbb{Z}^z\|, \quad (365)$$

and c is defined in Eq. (49). See Zozor, Bosyk, and Portesi (2014) for the explicit form of $B_{(\eta_1,\phi_1),(\eta_2,\phi_2)}(t)$. In general, this bound can be computed, since it involves only a one-parameter optimization over a bounded interval. Note that the functionals associated with the two terms in Eq. (364) may be different. This gives a very general result allowing one to consider Rényi entropy uncertainty relations that go beyond the usual conjugacy curve, defined by $1/\alpha+1/\beta=2$.

B. Certainty relations

Instead of lower bounding sums of entropies for different observables, one can also ask whether there exist nontrivial *upper* bounds on such sums. These bounds are called certainty relations. Of course, one would not expect to find nontrivial upper bounds for, say, the maximally mixed state $\rho_A=\mathbb{1}/d$. However, one might, e.g., restrict to pure states $|\psi\rangle_A$.

For some sets of observables, even restricting to pure states is not enough to get a certainty relation. For example, consider the Pauli σ_X and σ_Z observables for one qubit. One cannot find a certainty relation for these two observables because there exist states, namely, the eigenstates of σ_Y, that are unbiased with respect to the eigenbases of σ_X and σ_Z, and hence lead to maximum uncertainty in these two bases $H(X)+H(Z)=2$.

Recently Korzekwa, Jennings, and Rudolph (2014) proved a general result that nontrivial certainty relations are not possible for two arbitrary orthonormal bases $\mathbb{X}$ and $\mathbb{Z}$ in any finite dimension d. This follows from the fact that one can always find a pure state $|\psi\rangle_A$ that is unbiased with respect to both $\mathbb{X}$ and $\mathbb{Z}$.

However, a nontrivial certainty relation does exist, e.g., for a $d+1$ set of MUBs. This is connected to the fact that there are no states that are unbiased to all bases in a $d+1$ set of MUBs. Consider the result of Sánchez-Ruiz (1993), which deals with three MUBs ($\mathbb{X}$, $\mathbb{Y}$, and $\mathbb{Z}$) on a qubit system in a pure state:

$$H(X)+H(Y)+H(Z)\leq\frac{3}{2}\log 6-\frac{\sqrt{3}}{2}\log(2+\sqrt{3}). \quad (366)$$

The right-hand side of Eq. (366) is ≈ 2.23. Comparing this to the lower bound of 2, from Eq. (79), one sees that the allowable range for $H(X)+H(Y)+H(Z)$ is quite small. Sánchez-Ruiz (1993) noted that Eq. (366) is in fact the optimal certainty relation for these observables. More generally, considering a $d+1$ set of MUBs $\{\mathbb{X}_j\}$, Sánchez-Ruiz (1993) showed that

$$\sum_{j=1}^{n}H(X_j)\leq n\log(n+\sqrt{n})-\frac{1}{d}[n+(n-2)\sqrt{n}]\log(2+\sqrt{n}), \quad (367)$$

where $n=d+1$. Note that Eq. (366) is a special case of Eq. (367) corresponding to $d=2$.

Rastegin obtained some generalizations of Eq. (366) to the Rényi and Tsallis entropy families. In the Rényi case Rastegin (2014) found, for all $\alpha\in(0,1]$,

$$H_\alpha(X)+H_\alpha(Y)+H_\alpha(Z)\leq 3R_\alpha, \quad (368)$$

where

$$R_\alpha\coloneqq\frac{1}{1-\alpha}\log\left[\left(\frac{1+1/\sqrt{3}}{2}\right)^\alpha+\left(\frac{1-1/\sqrt{3}}{2}\right)^\alpha\right]. \quad (369)$$

Likewise Rastegin (2013a) found a similar sort of bound for the Tsallis entropies, but with $\log(x)$ in Eq. (369) replaced by $x-1$.

While these certainty relations are for MUBs, recently Puchała *et al.* (2015) studied a more general situation with sets of $n>2$ orthonormal bases in dimension d. Their certainty relations are upper bounds on the sum of Shannon entropies, similar to Eq. (367), but are not restricted to MUBs. Certainty relations for unitary k designs with $k=2$, 4 in terms of the mutual information were also covered by Matthews, Wehner, and Winter (2009).

Finally, it is worth reminding the reader that for the collision entropy one can obtain an *equality*, as in Eq. (82). An equation of this sort is both an uncertainty and a certainty relation. Stated another way, an equation implies that the strongest uncertainty relation coincides with the strongest certainty relation, leaving no gap between the two bounds. Equations such as (82) can, in turn, be used to derive certainty relations for other entropies, such as the min-entropy, due to the fact that $H_{\min}\leq H_2$.

The generalization of Eq. (82) to bipartite states ρ_{AB} was given in Eq. (185). Equation (185) is a certainty relation in the presence of quantum memory. It relates the amount of uncertainty to the amount of entanglement, as quantified by the conditional entropy $H_2(A|B)$. Similar to the unipartite case, Eq. (185) can be used to derive certainty relations (in the presence of quantum memory) for other entropies, such as the min-entropy, as discussed by Berta, Coles, and Wehner (2014).

Studying bipartite certainty relations in the presence of quantum memory is largely an open problem. For example, one could ask whether Eq. (366) or (367) can be appropriately generalized to the quantum memory case.

C. Measurement uncertainty

This review has focused on preparation uncertainty relations. Two other aspects of the uncertainty principle are (1) the

joint measurability of observable pairs and (2) the disturbance of one observable caused by the measurement of another observable. Joint measurability and measurement disturbance are two aspects of measurement uncertainty, which deals with fundamental restrictions on one's ability to measure things. For a detailed discussion of measurement uncertainty, see Ozawa (2003), Hall (2004), Busch, Heinonen, and Lahti (2007), and Busch, Lahti, and Werner (2014a). It is important, though, that we briefly mention measurement uncertainty here because the topic has seen significant debate recently (Busch, Lahti, and Werner, 2013, 2014a, 2014b). Rather than delve into the conceptual issues of measurement uncertainty, we simply give a few recent works that have taken an entropic approach, in particular, to measurement disturbance.

1. State-independent measurement-disturbance relations

One approach to measurement uncertainty is to ask how well can a measurement device perform on particular idealized sets of input states, e.g., the basis states associated with two complementary observables $\mathbb{X}$ and $\mathbb{Z}$? This is often called a state-independent approach, although it could also be called a calibration approach, since one is calibrating a device's performance based on idealized input states. For example, this approach was discussed by Busch, Lahti, and Werner (2013) for the position and momentum observables. However, the quantities in their relation were not entropic so we will not discuss it further.

More recently the calibration approach was taken by Buscemi *et al.* (2014) using entropic quantities. Consider a measurement apparatus represented by a quantum channel $\mathcal{M}$ acting on system A, and two counterfactual preparation schemes which will be fed into this apparatus, as shown in Fig. 19. In one scheme, A is prepared in a basis state of $\mathbb{X}$, say $|\mathbb{X}^x\rangle$, where the index x is chosen with uniformly random probability. The output of $\mathcal{M}$ consists of a classical system M as well as a "disturbed" version of the original quantum system A'. The classical output M represents an attempted measurement of the $\mathbb{X}$ observable, and it provides a guess for the index x. The measurement noise is then quantified by $\mathsf{N}(\mathcal{M},\mathbb{X}) \coloneqq H(X|M)$, where X is the random variable associated with the $\mathbb{X}$ observable on the input system, i.e., associated with the index x. In the other scheme, Fig. 19(b), A is prepared in a basis state of $\mathbb{Z}$, say $|\mathbb{Z}^z\rangle$, again with uniform probability. Now the question is can one recover a good guess of z from the outputs of $\mathcal{M}$? If not, then the interpretation is that the attempted measurement of $\mathbb{X}$ "disturbs" the $\mathbb{Z}$ observable. To quantify this, Buscemi *et al.* (2014) defined the disturbance of $\mathbb{Z}$ by $\mathsf{D}(\mathcal{M},\mathbb{Z}) \coloneqq \min_{\mathcal{R}} H(Z|\hat{Z})$. Here Z is the random variable associated with the observable $\mathbb{Z}$ on the input system, and $\mathcal{R}$ is a recovery map, i.e., a quantum channel that maps $A'M$ to a classical system $\hat{Z}$ that provides a guess for z. Their measurement-disturbance relation states that

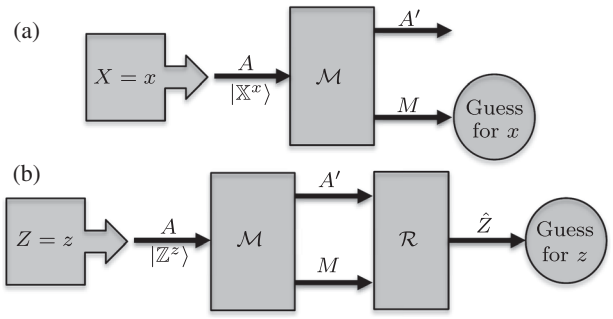


FIG. 19. Two scenarios considered by Buscemi *et al.* (2014), which capture (a) the noise of an attempted $\mathbb{X}$ measurement, and (b) the disturbance of the $\mathbb{Z}$ observable.

$$\mathsf{N}(\mathcal{M},\mathbb{X}) + \mathsf{D}(\mathcal{M},\mathbb{Z}) \geq q_{\mathrm{MU}}, \tag{370}$$

with q_{MU} as in Eq. (31). This shows a trade-off between the ability to measure the $\mathbb{X}$ states versus the ability to leave the $\mathbb{Z}$ states undisturbed.

Figure 19 is a dynamic scenario, similar to the scenario in Sec. IV.G. Hence, to derive Eq. (370), Buscemi *et al.* (2014) started with a "static" uncertainty relation (namely, the Maassen-Uffink relation) and then applied the static-dynamic isomorphism from Sec. IV.G.2. In particular, they employed the property in Eq. (247).

2. State-dependent measurement-disturbance relations

Now let us consider a sequential measurement scenario where system A is prepared in an arbitrary state ρ_A and fed into the measurement apparatus.

For simplicity, consider the sequential measurement of orthonormal bases, $\mathbb{X}$ followed by $\mathbb{Z}$, where the first measurement is a von Neumann measurement, i.e., it projects the system onto an $\mathbb{X}$-basis state. One can apply Maassen-Uffink's uncertainty relation to each outcome of the $\mathbb{X}$ measurement, i.e., to each state $|\mathbb{X}^x\rangle$, giving

$$H(Z)_{|\mathbb{X}^x\rangle} = H(X)_{|\mathbb{X}^x\rangle} + H(Z)_{|\mathbb{X}^x\rangle} \geq q_{\mathrm{MU}}. \tag{371}$$

Multiplying this by the probability $p^x = \langle \mathbb{X}^x|\rho_A|\mathbb{X}^x\rangle$ for outcome x, and summing over x gives

$$H(Z|X) \geq q_{\mathrm{MU}}, \tag{372}$$

where $H(Z|X)$ denotes the uncertainty for a future $\mathbb{Z}$ measurement given the outcome of the previous $\mathbb{X}$ measurement. Equation (372) was discussed in detail by Baek, Farrow, and Son (2014), and was also briefly mentioned by Coles and Piani (2014a). Note that Eq. (372) holds for any fixed input state ρ_A, and it is a state-dependent relation.

While Eq. (372) assumes the $\mathbb{X}$ measurement is an ideal von Neumann measurement, it is interesting to ask what happens if the first measurement is nonideal, i.e., a noisy measurement. There are various ways to address this. One approach, given by Coles and Furrer (2015), quantified the imperfection of the $\mathbb{X}$ measurement by the predictive error,

$$\mathsf{E}(\rho_A,\mathbb{X},\mathcal{E}) \coloneqq H_{\max}(X|M_X). \tag{373}$$

That is, the max-entropy of a future (perfect) $\mathbb{X}$ measurement given the register M_X that stores the outcome of the previous (imperfect) measurement of $\mathbb{X}$. Here $\mathcal{E}$, which maps

$A \to AM_X$, is the channel that performs this imperfect $\mathbb{X}$ measurement. One is interested in the disturbance of the $\mathbb{Z}$ observables caused by the imperfect $\mathbb{X}$ measurement. Coles and Furrer (2015) quantified the disturbance of $\mathbb{Z}$ using the Rényi relative entropies for $\alpha \in [1/2, \infty]$,

$$\mathsf{D}_\alpha(\rho_A, \mathbb{Z}, \mathcal{E}) \coloneqq D_\alpha(P_Z \| P_Z^{\mathcal{E}}). \tag{374}$$

Here P_Z is the initial probability distribution for the $\mathbb{Z}$ measurement and $P_Z^{\mathcal{E}}$ is the final probability distribution for $\mathbb{Z}$, i.e., after the imperfect $\mathbb{X}$ measurement. With these definitions, they found the measurement-disturbance relation

$$\mathsf{D}_\alpha(\rho_A, \mathbb{Z}, \mathcal{E}) + \mathsf{E}(\rho_A, \mathbb{X}, \mathcal{E}) + H_\alpha(Z)_P \geq q_{\mathrm{MU}}. \tag{375}$$

On the one hand, this gives a trade-off between measuring $\mathbb{X}$ well and causing large $\mathbb{Z}$ disturbance. On the other hand, the trade-off gets weaker as more initial uncertainty is contained in P_Z, as quantified by the term $H_\alpha(Z)_P$. So there is an interplay between initial uncertainty, measurement error, and disturbance.

VIII. PERSPECTIVES

We have discussed modern formulations of Heisenberg's uncertainty principle where uncertainty is quantified by entropy. Such formulations are directly relevant to quantum information-processing tasks as discussed in Sec. VI.

Technological applications such as QKD (Sec. VI.B) provide the driving force for obtaining more refined entropic uncertainty relations. For example, to prove security of QKD protocols involving more than two measurements, new entropic uncertainty relations are needed—namely, ones that allow for quantum memory and for multiple measurements. This is an important frontier that requires more research. Device-independent randomness, i.e., certifying randomness obtained from untrusted devices (Sec. VI.A.2) is another emerging application for which entropic uncertainty relations appear to be useful but more research is needed to find uncertainty relations that are specifically tailored to this application.

Aside from their technological applications, we believe that entropic uncertainty relations have a beauty to them. They give insight into the structure of quantum theory, and for that reason alone they are worth pursuing. For example, Sec. IV.F.5 noted a simple conjecture—that the sum of the mutual informations for two MUBs lower bounds the quantum mutual information.

New tools are being developed to prove entropic uncertainty relations. For example, the majorization approach (Sec. III.I) is promising. The relation between the majorization approach and the relative entropy approach (see Appendix B) remains to be clarified, and a unified framework would be insightful. For uncertainty relations with memory, Dupuis, Fawzi, and Wehner (2015) established a meta theorem to derive uncertainty relations. Yet, it is known that the resulting relations are not tight in all regimes, calling for further improvements.

One of the most exciting things about entropic uncertainty relations is that they give insight into basic physics. For example, Sec. VI.F discussed how entropic uncertainty relations allow one to unify the uncertainty principle with the wave-particle duality principle. A natural framework for quantifying wave-particle duality will likely come from applying entropic uncertainty relations to interferometers. Likewise, a hot topic in quantum foundations is measurement uncertainty. Section VII.C noted that entropic uncertainty relations may play an important role in obtaining conceptually clear formulations of measurement uncertainty. In that respect, very recently the notion of preparation uncertainty was combined with measurement reversibility (Berta, Wehner, and Wilde, 2016) and the corresponding entropic uncertainty relations were successfully tested on the IBM quantum experience (IBM, 2016).

Furthermore, entropic uncertainty relations will continue to help researchers characterize the boundary between separable versus entangled states (Sec. VI.D), as well as steerable versus nonsteerable states (Sec. VI.E).

Entropic uncertainty relations may play a role in the study of phase transitions in condensed matter physics (Romera and Calixto, 2015). Entropic uncertainty relations are also studied in the context of special and general relativity (Feng *et al.*, 2013; Jia, Tian, and Jing, 2015). Given that quantum information is playing an increasing role in cosmology (Hayden and Preskill, 2007), it would not be surprising to see future work on entropic uncertainty relations in the context of black hole physics.

ACKNOWLEDGMENTS

We thank Kais Abdelkhalek, Iwo Białynicki-Birula, Matthias Christandl, Rupert L. Frank, Gilad Gour, Michael J. W. Hall, Hans Maassen, Joseph M. Renes, Renato Renner, Lukasz Rudnicki, Christian Schaffner, Reinhard F. Werner, Mark M. Wilde, and Karol Zyczkowski for feedback. P. J. C. acknowledges support from Industry Canada, Sandia National Laboratories, NSERC Discovery Grant, and an Ontario Research Fund (ORF). M. B. acknowledges funding by the Swiss National Science Foundation (SNSF) through a fellowship, funding by the Institute for Quantum Information and Matter (IQIM), an NSF Physics Frontiers Center (NFS Grant No. PHY-1125565) with support of the Gordon and Betty Moore Foundation (No. GBMF-12500028), and funding support from the ARO grant for Research on Quantum Algorithms at the IQIM (No. W911NF-12-1-0521). M. T. is funded by a University of Sydney Postdoctoral Fellowship and acknowledges support from the ARC Centre of Excellence for Engineered Quantum Systems (EQUS). S. W. is supported by STW, Netherlands, an ERC Starting Grant QINTERNET, and an NWO VIDI grant.

APPENDIX A: MUTUALLY UNBIASED BASES

Section III.B defined MUBs and sets of n MUBs. The study of MUBs is closely related to the study of entropic uncertainty. Strong entropic uncertainty relations have been derived generically for sets of MUBs (particularly for $d+1$ sets of MUBs). Hence, constructing a new set of MUBs immediately yields a new entropic uncertainty relation. On the other hand, there is the interesting open question whether a set of n MUBs $\{\mathbb{X}_j\}$ yields the strongest bound b in a generic uncertainty relation of the form

$$\sum_{j=1}^{n} H(X_j) \geq b. \tag{A1}$$

A review of MUBs has been given by Durt *et al.* (2010). Here we discuss the connection of MUBs to Hadamard matrices, as well as the existence and construction of MUBs.

1. Connection to Hadamard matrices

Any two orthonormal bases are related by a unitary, and in the case of MUBs, that unitary is called a Hadamard matrix H. The general form of such matrices is

$$H = \sum_{j,k} \frac{e^{i\phi_{jk}}}{\sqrt{d}} |j\rangle\langle k|, \tag{A2}$$

where the phase factors ϕ_{jk} must be appropriately chosen so that H is unitary. Notice that each matrix element has a magnitude of $1/\sqrt{d}$, which is the defining property of Hadamard unitaries. The best known Hadamard is the Fourier matrix, defined in Eq. (204),

$$F = \sum_{j,k} \frac{\omega^{-jk}}{\sqrt{d}} |j\rangle\langle k|, \tag{A3}$$

with $\omega = e^{2\pi i/d}$, which relates the generalized Pauli operators

$$\sigma_{\mathbb{Z}} = \sum_j \omega^j |j\rangle\langle j|, \qquad \sigma_{\mathbb{X}} = F\sigma_{\mathbb{Z}}F^{\dagger} = \sum_j |j+1\rangle\langle j|. \tag{A4}$$

For $d = 2$ these are just the usual Pauli matrices from example 7.

It should be clear that the problem of finding MUBs is equivalent to the problem of finding Hadamard matrices. We note that Hadamard matrices can be categorized into equivalence classes, based on whether there exists a diagonal unitary or permutation that maps one Hadamard to another. A detailed catalog of Hadamard matrices can be found online (Bruzda, Tadej, and Życzkowski, 2015).

2. Existence

That there exist MUB pairs in any finite dimension follows from the fact that we can write down the Fourier matrix in Eq. (A3) for any d. In fact, for any d there exists a set of three MUBs, e.g., formed from the eigenvectors of $\sigma_{\mathbb{X}}$, $\sigma_{\mathbb{Z}}$, and $\sigma_{\mathbb{X}}\sigma_{\mathbb{Z}}$. It is also known that a set of MUBs can at most be of size $d+1$ (Bandyopadhyay, Roychowdhury, and Vatan, 2002). Such $d+1$ sets are called complete sets of MUBs. Complete sets play a role in tomography since they are informationally complete, and they have the useful property of forming a complex projective two-design (Klappenecker and Rotteler, 2005). Complete sets of MUBs are known to exist in prime power dimensions, i.e., $d = p^m$, where p is a prime and m is a positive integer (Bandyopadhyay, Roychowdhury, and Vatan, 2002). However, even for the smallest number that is not a prime power, namely 6, the existence problem remains unsolved.

3. Simple constructions

When d is a prime, a simple construction (Wootters and Fields, 1989; Bandyopadhyay, Roychowdhury, and Vatan, 2002) of a complete set of MUBs is to consider the eigenvectors of the $d+1$ products of the form

$$\{\sigma_{\mathbb{Z}}, \sigma_{\mathbb{X}}, \sigma_{\mathbb{X}}\sigma_{\mathbb{Z}}, \sigma_{\mathbb{X}}\sigma_{\mathbb{Z}}^2, \ldots, \sigma_{\mathbb{X}}\sigma_{\mathbb{Z}}^{d-1}\}. \tag{A5}$$

More generally for $d = p^m$, a construction is known where each basis B_i comes from the common eigenvectors of a corresponding set C_i of commuting matrices (Bandyopadhyay, Roychowdhury, and Vatan, 2002). The elements of C_i are a subset of size $|C_i| = d-1$ of the d^2-1 Pauli products $\sigma_{\mathbb{X}}^j\sigma_{\mathbb{Z}}^k$ (excluding the identity). The subset is chosen such that all the elements of C_i commute and $C_i \bigcap C_j = \{\mathbb{1}\}$ for $i \neq j$.

APPENDIX B: PROOF OF MAASSEN-UFFINK'S RELATION

Here we give a proof of Maassen-Uffink's uncertainty relation for the Shannon entropy (31). Our proof closely follows the ideas of Coles *et al.* (2012) and makes use of the data-processing inequality for the relative entropy (Lieb and Ruskai, 1973; Lindblad, 1975; Uhlmann, 1977). In fact, we will prove the slightly stronger relation stated in Eq. (47):

$$H(X) + H(Z) \geq \log\frac{1}{c} + H(\rho_A). \tag{B1}$$

Proof. For the proof of Eq. (B1) we consider the classical state $\rho_X = \mathcal{X}_{A\to X}(\rho_A)$ generated by applying the measurement map

$$\mathcal{X}_{A\to X}(\cdot) = \sum_x |\mathbb{X}^x\rangle\langle\mathbb{X}^x| \cdot |\mathbb{X}^x\rangle\langle\mathbb{X}^x|, \tag{B2}$$

where the auxiliary Hilbert space X allows us to represent the classical random variable X in the quantum formalism.

It is easy to verify that the Shannon entropy of the distribution P_X is equal to the von Neumann entropy of the state ρ_X. From this we get

$$H(X) = -\mathrm{tr}[\rho_X \log \rho_X] = -\mathrm{tr}[\mathcal{X}(\rho_A) \log \mathcal{X}(\rho_A)] \tag{B3}$$

$$= -\mathrm{tr}[\rho_A \log \mathcal{X}(\rho_A)], \tag{B4}$$

where the last equality is straightforward to check by writing out the trace and the measurement map $\mathcal{X}_{A\to X}$. By phrasing the right-hand side of Eq. (B3) in terms of relative entropy $D(\rho\|\sigma) = \mathrm{tr}[\rho(\log\rho - \log\sigma)]$, we arrive at

$$H(X) = D(\rho_A\|\mathcal{X}(\rho_A)) + H(\rho_A). \tag{B5}$$

We then apply the measurement map

$$\mathcal{Z}_{A\to Z}(\cdot) = \sum_z |\mathbb{Z}^z\rangle\langle\mathbb{Z}^z| \cdot |\mathbb{Z}^z\rangle\langle\mathbb{Z}^z| \tag{B6}$$

to both arguments of the relative entropy, and find by the data-processing inequality for the relative entropy that

$$D(\rho_A\|\mathcal{X}(\rho_A)) \geq D(\mathcal{Z}(\rho_A)\|\mathcal{Z}\circ\mathcal{X}(\rho_A)) \tag{B7}$$

$$= D(\rho_Z\|\mathcal{Z}\circ\mathcal{X}(\rho_A)), \tag{B8}$$

where $\rho_Z = \mathcal{Z}_{A\to Z}(\rho_A)$. By writing out both measurement maps we find the classical state

$$\mathcal{Z}\circ\mathcal{X}(\rho_A) = \sum_z |\mathbb{Z}^z\rangle\langle\mathbb{Z}^z| \cdot \sum_x |\langle\mathbb{X}^x|\mathbb{Z}^z\rangle|^2 \langle\mathbb{X}^x|\rho_A|\mathbb{X}^x\rangle, \tag{B9}$$

and the right-hand side of Eq. (B7) becomes

$$D(\rho_Z\|\mathcal{Z}\circ\mathcal{X}(\rho_A)) = -H(\rho_Z) - \sum_z \langle\mathbb{Z}^z|\rho_A|\mathbb{Z}^z\rangle \times \log\left(\sum_x |\langle\mathbb{X}^x|\mathbb{Z}^z\rangle|^2 \langle\mathbb{X}^x|\rho_A|\mathbb{X}^x\rangle\right). \tag{B10}$$

Now the logarithm is a monotonic function and hence we find

$$-\sum_z \langle\mathbb{Z}^z|\rho_A|\mathbb{Z}^z\rangle \log\left(\sum_x |\langle\mathbb{X}^x|\mathbb{Z}^z\rangle|^2 \langle\mathbb{X}^x|\rho_A|\mathbb{X}^x\rangle\right) \geq -\sum_z \langle\mathbb{Z}^z|\rho_A|\mathbb{Z}^z\rangle \log\left(\max_{x',z'} |\langle\mathbb{X}^{x'}|\mathbb{Z}^{z'}\rangle|^2 \sum_x \langle\mathbb{X}^x|\rho_A|\mathbb{X}^x\rangle\right) \tag{B11}$$

$$= -\log \max_{x',z'} |\langle\mathbb{X}^{x'}|\mathbb{Z}^{z'}\rangle|^2. \tag{B12}$$

By combining Eqs. (B3)–(B12) and noting that $H(Z)$ equals the von Neumann entropy of ρ_Z, we arrive at the claim (B1). ∎

APPENDIX C: RÉNYI ENTROPIES FOR JOINT QUANTUM SYSTEMS

Here we define general conditional Rényi entropies. This allows us to exhibit their intuitive properties in a general setting without having to discuss various special cases individually. We exhibit these properties to show a generalization of the Maassen-Uffink relation to the tripartite quantum memory setting.

1. Definitions

For any bipartite quantum state ρ_{AB} and $\alpha \in [\frac{1}{2}, \infty]$, we define the quantum conditional Rényi entropy as

$$H_\alpha(A|B) := -\min_{\sigma_B} D_\alpha(\rho_{AB}\|\mathbb{1}_A \otimes \sigma_B), \tag{C1}$$

where σ_B is a quantum state on B. Here D_α is the Rényi divergence of order α (Müller-Lennert *et al.*, 2013; Wilde, Winter, and Yang, 2014), namely,[36]

$$D_\alpha(\rho\|\sigma) := \frac{1}{\alpha-1}\log \mathrm{tr}[(\sigma^{(1-\alpha)/2\alpha}\rho\sigma^{(1-\alpha)/2\alpha})^\alpha] \quad \text{for } \alpha \in \left[\frac{1}{2}, 1\right)\cup(1,\infty) \tag{C2}$$

and as the corresponding limit for $\alpha \in \{1, \infty\}$. These divergences are measures of distinguishability between quantum states and some of their properties are discussed in Appendix C.2. Note the following special cases that we previously encountered. First, the conditional min- and max-entropies are simply recovered as $H_{\min} \equiv H_\infty$ and $H_{\max} \equiv H_{1/2}$. The conditional von Neumann entropy is recovered as $H \equiv H_1$. Finally, the conditional collision entropy can be expressed as

$$H_{\mathrm{coll}}(A|B) = -D_2(\rho_{AB}\|\mathbb{1}_A \otimes \rho_B). \tag{C3}$$

Note that $H_2(A|B) \leq H_{\mathrm{coll}}(A|B)$ since the former involves a minimization over marginal states σ_B. The two expressions are not equal in general and we want to mostly work with $H_{\mathrm{coll}}(A|B)$ because it has the operational interpretation as in Eqs. (139) and (148).

2. Entropic properties

We present the properties for the whole family of Rényi divergences and entropies, but recall that the properties also apply to the relative entropy and the von Neumann entropy as special cases. Most properties of the conditional Rényi entropy can be derived from properties of the underlying Rényi divergence.[37]

a. Positivity and monotonicity

First we remark that $D_\alpha(\rho\|\sigma)$ is guaranteed to be nonnegative when the arguments ρ and σ are normalized, and $D_\alpha(\rho\|\sigma) = 0$ when $\rho = \sigma$. Also, $\alpha \mapsto D_\alpha(\rho\|\sigma)$ is monotonically increasing in α. Thus, for any $\beta \geq \alpha$, we have

$$0 \leq D_\alpha(\rho\|\sigma) \leq D_\beta(\rho\|\sigma), \tag{C4}$$

and

$$\log d_A \geq H_\alpha(A|B) \geq H_\beta(A|B) \geq -\log\min\{d_A, d_B\}. \tag{C5}$$

This means that the conditional Rényi entropies, in particular, also the conditional von Neumann entropy, can be negative. However, this can happen only in the presence of quantum entanglement and the conditional entropies are thus always positive when one of the two systems is classical. The maximum $\log d_A$ is achieved for a state of the form $\rho_{AB} = \mathbb{1}_A/d_A \otimes \rho_B$. On the other hand, the minimum $-\log d_A$ is achieved for the maximally entangled pure state

[36] This quantum generalization is not unique—in fact other generalizations based on Petz's notion of Rényi divergence (Ohya and Petz, 1993) have also been explored, for example, by Tomamichel, Berta, and Hayashi (2014). However, for this review it is convenient to stick with the proposed definition in Eqs. (C1) and (C2) as it entails the most important special cases encountered here and in the literature.

[37] These divergences were investigated in a series of recent works (Beigi, 2013; Frank and Lieb, 2013b; Müller-Lennert *et al.*, 2013; Wilde, Winter, and Yang, 2014; Mosonyi and Ogawa, 2015) and proofs of the properties discussed here can be found in these references.

$$|\psi\rangle_{AB} = \frac{1}{\sqrt{d_A}} \sum_x |x\rangle_A \otimes |x\rangle_B.$$

b. Data-processing inequalities

Any quantum channel is described by a completely positive and trace-preserving (CPTP) map. The Rényi divergences satisfy a data-processing inequality. Namely, for all $\alpha \geq 1/2$ and any CPTP map $\mathcal{E}$, we find the following relation (Frank and Lieb, 2013b):

$$D_\alpha(\mathcal{E}(\rho)\|\mathcal{E}(\sigma)) \leq D_\alpha(\rho\|\sigma). \tag{C6}$$

This is an expression of the intuitive property that it is easier to distinguish between the inputs rather than the outputs of any quantum channel. In fact, this property holds more generally for any completely positive trace nonincreasing map $\mathcal{E}$ which satisfies $\mathrm{tr}[\mathcal{E}(\rho)] = 1$. This has two important implications for conditional entropies. First, consider an arbitrary CPTP map $\mathcal{E}_{B\to B'}$ acting on the side information that takes ρ_{AB} to $\tau_{AB'} = \mathcal{I}_A \otimes \mathcal{E}_{B\to B'}(\rho_{AB})$. Then we have $H_\alpha(A|B) \leq H_\alpha(A|B')$. This tells us that any physically allowed information processing of the side information B may only increase the uncertainty we have about A.

Example 35. An often encountered special case of the data-processing inequality is that $H_\alpha(A|BC) \leq H_\alpha(A|B)$ for any tripartite state ρ_{ABC}. This expresses the fact that throwing away part of the side information can only increase the uncertainty about A.

The second application concerns rank-one projective measurements on the A system. More precisely, we consider any rank-one projective measurement $\mathcal{X}_{A\to X}$ that takes ρ_{AB} to

$$\rho_{XB} = \mathcal{X}_{A\to X} \otimes \mathcal{I}_B(\rho_{AB}) \tag{C7}$$

$$= \sum_x (|\mathbb{X}^x\rangle\langle\mathbb{X}^x|_A \otimes \mathbb{1}_B)\rho_{AB}(|\mathbb{X}^x\rangle\langle\mathbb{X}^x|_A \otimes \mathbb{1}_B). \tag{C8}$$

Then we find that $H_\alpha(A|B) \leq H_\alpha(X|B)$, which reveals that measuring out system A completely can only increase the uncertainty we have about it.[38]

c. Duality and additivity

We see that the following property is essential for deriving uncertainty relations with quantum side information. For any tripartite state ρ_{ABC}, the conditional Rényi entropies satisfy the following *duality relation*. For $\alpha, \beta \in [1/2, \infty]$ such that $1/\alpha + 1/\beta = 2$, we have (Beigi, 2013; Müller-Lennert *et al.*, 2013)

$$H_\alpha(A|B) + H_\beta(A|C) \geq 0, \tag{C9}$$

with equality if ρ_{ABC} is pure.

This is a quantitative manifestation of the monogamy of quantum correlations. For example, if system A is highly entangled with system B we find that the conditional von Neumann entropy $H(A|B)$ is negative. However, the duality relation (C9) now shows that for any third system C correlated with A and B, it holds that $H(A|C) \geq -H(A|B)$; that is, the uncertainty of A from an observer with access to C is necessarily large in this case.

The Rényi entropies are additive. Namely, given a product state of the form $\rho_{ABCD} = \rho_{AC} \otimes \rho_{BD}$, they satisfy $H_\alpha(AB|CD) = H_\alpha(A|C) + H_\alpha(B|D)$. This is in fact a consequence of the duality relation.[39]

3. Axiomatic proof of uncertainty relation with quantum memory

Here we give a concise proof of the generalized Maassen-Uffink relation (221),

$$H_\alpha(X|B)_\rho + H_\beta(Z|C) \geq q_{\mathrm{MU}}, \tag{C10}$$

where $1/\alpha + 1/\beta = 2$. Note that the proof applies to a general class of entropic quantities that satisfy certain properties, but we specialize it here to conditional Rényi entropies.

Let us consider measurements $\mathbb{X} = \{\mathbb{X}_A^x\}$ and $\mathbb{Z} = \{\mathbb{Z}_A^z\}$ in two orthonormal bases such that $\mathbb{X}_A^x$ and $\mathbb{Z}_A^z$ are rank-one projectors. The proof for POVMs follows essentially the same steps, as detailed by Coles *et al.* (2012) [based on ideas of Coles *et al.* (2011) and Tomamichel and Renner (2011)].

Proof of (C10). First let us define the isometry $V := \sum_z |z\rangle_Z \otimes \mathbb{Z}_A^z$ associated with the $\mathbb{Z}$ measurement on system A, and the state $\tilde{\rho}_{ZABC} := V\rho_{ABC}V^\dagger$. We find the following sequence of inequalities:

$$H_\beta(Z|C) \geq -H_\alpha(Z|AB) \tag{C11}$$

$$= \min_{\sigma_{AB}} D_\alpha(\tilde{\rho}_{ZAB}\|\mathbb{1}_Z \otimes \sigma_{AB}) \tag{C12}$$

$$\geq \min_{\sigma_{AB}} D_\alpha\left(\rho_{AB}\Big\|\sum_z \mathbb{Z}_A^z \sigma_{AB} \mathbb{Z}_A^z\right) \tag{C13}$$

$$\geq \min_{\sigma_{AB}} D_\alpha\left(\bar{\rho}_{XB}\Big\|\sum_{x,z} |\langle\mathbb{X}_A^x|\mathbb{Z}_A^z\rangle|^2 \mathbb{X}_A^x \otimes \mathrm{tr}_A[\mathbb{Z}_A^z \sigma_{AB}]\right), \tag{C14}$$

where we used $\bar{\rho}_{XB} := \sum_k \mathbb{X}_A^x \rho_{AB} \mathbb{X}_A^x$. To establish Eq. (C11), we applied the duality relation (C9) to the state $\tilde{\rho}_{ZABC}$. Equation (C12) is simply the definition of the conditional entropy as in Eq. (C1). To find (C13), we apply the data-processing inequality for the partial isometry $V^\dagger$ as a trace nonincreasing map, and note that $V^\dagger(\mathbb{1}_Z \otimes \sigma_{AB})V = \sum_z \mathbb{Z}_A^z \sigma_{AB} \mathbb{Z}_A^z$. Next Eq. (C14) follows by applying the

[38] The inequality holds more generally for all CPTP maps on $\mathcal{E}_{A\to A'}$ that satisfy $\mathcal{E}_{A\to A'}(\mathbb{1}_A) = \mathbb{1}_{A'}$ (unital maps).

[39] Recall that by definition (C1), we have

$$\begin{aligned} H_\alpha(AB|CD) &= -\min_{\sigma_{CD}} D_\alpha(\rho_{ABCD}\|\mathbb{1}_{AB} \otimes \sigma_{CD}) \\ &\geq -\min_{\sigma_C, \sigma_D} D_\alpha(\rho_{ABCD}\|\mathbb{1}_{AB} \otimes \sigma_C \otimes \sigma_D) \\ &= H_\alpha(A|C) + H_\alpha(B|D). \end{aligned}$$

The reverse inequality then follows due to the duality relation.

data-processing inequality for the measurement CPTP map $\mathcal{X}(\cdot) = \sum_x \mathbb{X}^x \cdot \mathbb{X}^x$.

Next we observe that

$$\sum_{x,z} |\langle \mathbb{X}_A^x | \mathbb{Z}_A^z \rangle|^2 \mathbb{X}_A^x \otimes \mathrm{tr}_A[\mathbb{Z}_A^z \sigma_{AB}] \leq c \sum_{x,z} \mathbb{X}_A^x \otimes \mathrm{tr}_A[\mathbb{Z}_A^z \sigma_{AB}] = c \mathbb{1}_A \otimes \sigma_B, \quad \text{(C15)}$$

where we recall that $c = \max_{x,z} |\langle \mathbb{X}_A^x | \mathbb{Z}_A^z \rangle|^2$ as defined in Eq. (32). Moreover, we need that for any σ' and positive λ such that $\sigma \leq \lambda \sigma'$, we have $D_\alpha(\rho\|\sigma) \geq D_\alpha(\rho\|\sigma') + \log(1/\lambda)$.[40] Continuing from Eq. (C14), we thus find that

$$H_\beta(Z|C) \geq \min_{\sigma_B} D_\alpha(\bar{\rho}_{XB} \| \mathbb{1}_X \otimes \sigma_B) + q_{\mathrm{MU}} \quad \text{(C16)}$$

$$= -H_\alpha(X|B) + q_{\mathrm{MU}}, \quad \text{(C17)}$$

where (C17) again follows by the definition of the conditional entropy. ∎

[40]For a proof of this property, see Müller-Lennert *et al.* (2013), Prop. 4.

REFERENCES

Abdelkhalek, K., R. Schwonnek, H. Maassen, F. Furrer, J. Duhme, P. Raynal, B.-G. Englert, and R. F. Werner, 2015, Int. J. Quantum. Inform. **13**, 1550045.

Adamczak, R., R. Latała, Z. Puchała, and K. Życzkowski, 2016, J. Math. Phys. (N.Y.) **57**, 032204.

Ambainis, A., 2010, Quantum Inf. Comput. **10**, 0848.

Azarchs, A., 2004, Entropic Uncertainty Relations for Incomplete Sets of Mutually Unbiased Observables, semester thesis (California Institute of Technology).

Baek, K., T. Farrow, and W. Son, 2014, Phys. Rev. A **89**, 032108.

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

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

Bandyopadhyay, S., P. O. BoykinV. Roychowdhury, and F. Vatan, 2002, Algorithmica **34**, 512.

Barnum, H., and E. Knill, 2002, J. Math. Phys. (N.Y.) **43**, 2097.

Baumgratz, T., M. Cramer, and M. B. Plenio, 2014, Phys. Rev. Lett. **113**, 140401.

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

Beigi, S., 2013, J. Math. Phys. (N.Y.) **54**, 122202.

Bennett, C. H., and G. Brassard, 1984, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing 1984*, Vol. 1 (IEEE, Bangalore), pp. 175–179.

Bergh, J., and J. Löfström, 1976, *Interpolation Spaces, Grundlehren der mathematischen Wissenschaften*, Vol. 223 (Springer, Berlin/Heidelberg).

Berta, M., 2013, Quantum Side Information: Uncertainty Relations, Extractors, Channel Simulations, Ph.D. thesis (ETH, Zurich).

Berta, M., F. G. S. L. Brandao, M. Christandl, and S. Wehner, 2013, IEEE Trans. Inf. Theory **59**, 6779.

Berta, M., M. Christandl, R. Colbeck, J. M. Renes, and R. Renner, 2010, Nat. Phys. **6**, 659.

Berta, M., P. J. Coles, and S. Wehner, 2014, Phys. Rev. A **90**, 062127.

Berta, M., O. Fawzi, and S. Wehner, 2014, IEEE Trans. Inf. Theory **60**, 1168.

Berta, M., S. Wehner, and M. M. Wilde, 2016, New J. Phys. **18**, 073004.

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

Białynicki-Birula, I., 2006, Phys. Rev. A **74**, 052101.

Białynicki-Birula, I., 2007, in *AIP Conference Proceedings*, Vol. 889 (AIP, Vaxjo), pp. 52–61.

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

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

Białynicki-Birula, I., and Ł. Rudnicki, 2011, in *Statistical Complexity*, edited by K. Sen (Springer Netherlands, Dordrecht), pp. 1–34.

Biham, E., M. Boyer, P. O. Boykin, T. Mor, and V. Roychowdhury, 2000, in *Proc. ACM STOC 2000* (ACM Press, New York), pp. 715–724.

Biham, E., M. Boyer, P. O. Boykin, T. Mor, and V. Roychowdhury, 2006, J. Cryptol. **19**, 381.

Boltzmann, L., 1872, in *Sitzungsberichte der Akademie der Wissenschaften zu Wien*, Vol. 66, pp. 275–370.

Bosyk, G. M., M. Portesi, F. Holik, and A. Plastino, 2013, Phys. Scr. **87**, 065002.

Broadbent, A., and C. Schaffner, 2016, Des. Codes Cryptogr. **78**, 351.

Brukner, Ć., and A. Zeilinger, 1999, Phys. Rev. Lett. **83**, 3354.

Bruß, D., 1998, Phys. Rev. Lett. **81**, 3018.

Bruzda, W., W. Tadej, and K. Życzkowski, 2015, "Complex Hadamard Matrices," http://chaos.if.uj.edu.pl/%7Ekarol/hadamard/index.php

Buhrman, H., M. Christandl, P. Hayden, H.-K. Lo, and S. Wehner, 2008, Phys. Rev. A **78**, 022316.

Buscemi, F., M. J. W. Hall, M. Ozawa, and M. M. Wilde, 2014, Phys. Rev. Lett. **112**, 050401.

Busch, P., T. Heinonen, and P. Lahti, 2007, Phys. Rep. **452**, 155.

Busch, P., P. Lahti, and R. F. Werner, 2013, Phys. Rev. Lett. **111**, 160405.

Busch, P., P. Lahti, and R. F. Werner, 2014a, Rev. Mod. Phys. **86**, 1261.

Busch, P., P. Lahti, and R. F. Werner, 2014b, Phys. Rev. A **89**, 012129.

Busch, P., and C. Shilladay, 2006, Phys. Rep. **435**, 1.

Cachin, C., and U. Maurer, 1997, in *Proceedings of CRYPTO 1997*, LNCS, Vol. 1294 (Springer, New York), pp. 292–306.

Canetti, R., 2001, in *Proc. IEEE FOCS 2001* (IEEE, New York), pp. 136–145.

Cavalcanti, E. G., S. J. Jones, H. M. Wiseman, and M. D. Reid, 2009, Phys. Rev. A **80**, 032112.

Cerf, N. J., M. Bourennane, A. Karlsson, and N. Gisin, 2002, Phys. Rev. Lett. **88**, 127902.

Chen, B., and S.-M. Fei, 2015, Quantum Inf. Process. **14**, 2227.

Choi, M., 1975, Linear Algebra Appl. **10**, 285.

Christandl, M., and A. Winter, 2005, IEEE Trans. Inf. Theory **51**, 3159.

Coles, P. J., 2012a, Phys. Rev. A **86**, 062334.

Coles, P. J., 2012b, Phys. Rev. A **85**, 042103.

Coles, P. J., R. Colbeck, L. Yu, and M. Zwolak, 2012, Phys. Rev. Lett. **108**, 210405.

Coles, P. J., and F. Furrer, 2015, Phys. Lett. A **379**, 105.

Coles, P. J., J. Kaniewski, and S. Wehner, 2014, Nat. Commun. **5**, 5814.

Coles, P. J., and M. Piani, 2014a, Phys. Rev. A **89**, 010302.

Coles, P. J., and M. Piani, 2014b, Phys. Rev. A **89**, 022112.

Coles, P. J., L. Yu, V. Gheorghiu, and R. Griffiths, 2011, Phys. Rev. A **83**, 062338.

Damgaard, I. B., S. Fehr, R. Renner, L. Salvail, and C. Schaffner, 2007, in *Proceedings of CRYPTO 2007*, LNCS, Vol. 4622 (Springer, New York), pp. 360–378.

Damgaard, I. B., S. Fehr, L. Salvail, and C. Schaffner, 2008, SIAM J. Comput. **37**, 1865.

Dammeier, L., R. Schwonnek, and R. F. Werner, 2015, New J. Phys. **17**, 093046.

Dankert, C., R. Cleve, J. Emerson, and E. Livine, 2009, Phys. Rev. A **80**, 012304.

Davies, E. B., 1976, *Quantum Theory of Open Systems* (Academic Press, New York).

del Rio, L., J. Aberg, R. Renner, O. Dahlsten, and V. Vedral, 2011, Nature (London) **474**, 61.

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

Devetak, I., and A. Winter, 2003, Phys. Rev. A **68**, 042301.

Devetak, I., and A. Winter, 2005, Proc. R. Soc. A **461**, 207.

de Vicente, J., and J. Sánchez-Ruiz, 2008, Phys. Rev. A **77**, 042110.

Dey, A., T. Pramanik, and A. S. Majumdar, 2013, Phys. Rev. A **87**, 012120.

Dietz, K., 2006, J. Phys. A **39**, 1433.

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

Dupuis, F., O. Fawzi, and S. Wehner, 2015, IEEE Trans. Inf. Theory **61**, 1093.

Dupuis, F., J. Florjanczyk, P. Hayden, and D. Leung, 2013, Proc. R. Soc. A **469**, 20130289.

Dürr, S., and G. Rempe, 2000, Am. J. Phys. **68**, 1021.

Durt, T., B.-G. Englert, I. Bengtsson, and K. Życzkowski, 2010, Int. J. Quantum. Inform. **08**, 535.

Dziembowski, S., and U. Maurer, 2004, in *Proceedings of EUROCRYPT 2004*, LNCS, Vol. 3027 (Springer, New York), pp. 126–137.

Eberle, T., V. Händchen, and R. Schnabel, 2013, Opt. Express **21**, 11546.

Einstein, A., B. Podolsky, and N. Rosen, 1935, Phys. Rev. **47**, 777.

Ekert, A. K., 1991, Phys. Rev. Lett. **67**, 661.

Englert, B.-G., 1996, Phys. Rev. Lett. **77**, 2154.

Englert, B.-G., and J. A. Bergou, 2000, Opt. Commun. **179**, 337.

Englert, B.-G., D. Kaszlikowski, L. C. Kwek, and W. H. Chee, 2008, Int. J. Quantum. Inform. **06**, 129.

Everett, H., 1957, Rev. Mod. Phys. **29**, 454.

Fawzi, O., P. Hayden, and P. Sen, 2011, in *Proceedings of ACM STOC 2011* (ACM Press, New York), pp. 773–782.

Feng, J., Y.-Z. Zhang, M. D. Gould, and H. Fan, 2013, Phys. Lett. B **726**, 527.

Frank, R. L., and E. H. Lieb, 2012, Ann. Henri Poincaré **13**, 1711.

Frank, R. L., and E. H. Lieb, 2013a, Commun. Math. Phys. **323**, 487.

Frank, R. L., and E. H. Lieb, 2013b, J. Math. Phys. (N.Y.) **54**, 122201.

Friedland, S., V. Gheorghiu, and G. Gour, 2013, Phys. Rev. Lett. **111**, 230401.

Furrer, F., J. Aberg, and R. Renner, 2011, Commun. Math. Phys. **306**, 165.

Furrer, F., M. Berta, M. Tomamichel, V. B. Scholz, and M. Christandl, 2014, J. Math. Phys. (N.Y.) **55**, 122205.

Furrer, F., T. Franz, M. Berta, A. Leverrier, V. B. Scholz, M. Tomamichel, and R. F. Werner, 2012, Phys. Rev. Lett. **109**, 100502.

Gavinsky, D., J. Kempe, I. Kerenidis, R. Raz, and R. de Wolf, 2009, SIAM J. Comput. **38**, 1695.

Gehring, T., V. Händchen, J. Duhme, F. Furrer, T. Franz, C. Pacher, R. F. Werner, and R. Schnabel, 2015, Nat. Commun. **6**, 8795.

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

Gibbs, J. W., 1878, Am. J. Sci. **s3-16**, 441.

Giovannetti, V., 2004, Phys. Rev. A **70**, 012102.

Giovannetti, V., S. Lloyd, and L. Maccone, 2011, Nat. Photonics **5**, 222.

Grosshans, F., and N. J. Cerf, 2004, Phys. Rev. Lett. **92**, 047905.

Grudka, A., M. Horodecki, P. Horodecki, R. Horodecki, W. Klobus, and L. Pankowski, 2013, Phys. Rev. A **88**, 032106.

Guha, S., P. Hayden, H. Krovi, S. Lloyd, C. Lupo, J. H. Shapiro, M. Takeoka, and M. M. Wilde, 2014, Phys. Rev. X **4**, 011016.

Gühne, O., and M. Lewenstein, 2004, Phys. Rev. A **70**, 022316.

Gühne, O., and G. Tóth, 2009, Phys. Rep. **474**, 1.

Hall, M. J. W., 1993, J. Mod. Opt. **40**, 809.

Hall, M. J. W., 1994, Phys. Rev. A **49**, 42.

Hall, M. J. W., 1995, Phys. Rev. Lett. **74**, 3307.

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

Hall, M. J. W., 1999, Phys. Rev. A **59**, 2602.

Hall, M. J. W., 2004, Phys. Rev. A **69**, 052113.

Hall, M. J. W., 2008, J. Phys. A **41**, 255301.

Hall, M. J. W., D. W. Berry, M. Zwierz, and H. M. Wiseman, 2012, Phys. Rev. A **85**, 041802.

Hall, M. J. W., and H. M. Wiseman, 2012, New J. Phys. **14**, 033040.

Hausladen, P., and W. K. Wootters, 1994, J. Mod. Opt. **41**, 2385.

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

Hayden, P., and J. Preskill, **2007**, J. High Energy Phys. 09, 120.

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

Hiai, F., and D. Petz, 1991, Commun. Math. Phys. **143**, 99.

Hirschman, I. I., 1957, Am. J. Math. **79**, 152.

Holevo, A. S., 1973, Probl. Inf. Transm. **9**, 177 [http://www.mathnet.ru/php/archive.phtml?wshow=paper&jrnid=ppi&paperid=903&option_lang=eng].

Horodecki, M., J. Oppenheim, and A. Winter, 2006, Commun. Math. Phys. **269**, 107.

Horodecki, R., P. Horodecki, M. Horodecki, and K. Horodecki, 2009, Rev. Mod. Phys. **81**, 865.

Hu, M.-L., and H. Fan, 2012, Phys. Rev. A **86**, 032338.

Hu, M.-L., and H. Fan, 2013a, Phys. Rev. A **87**, 022314.

Hu, M.-L., and H. Fan, 2013b, Phys. Rev. A **88**, 014105.

Huang, Y., 2010, Phys. Rev. A **82**, 012335.

Huang, Y., 2011, Phys. Rev. A **83**, 052124.

Huang, Y., 2013, IEEE Trans. Inf. Theory **59**, 6774.

IBM, 2016, "IBM quantum experience."

Impagliazzo, R., L. A. Levin, and M. Luby, 1989, in *Proceedings of ACM STOC 1989* (ACM, New York), pp. 12–24.

Impagliazzo, R., and D. Zuckerman, 1989, in *Proceedings of IEEE FOCS 1989* (IEEE, New York), pp. 248–253.

Ivanovic, I. D., 1992, J. Phys. A **25**, L363.

Jaeger, G., A. Shimony, and L. Vaidman, 1995, Phys. Rev. A **51**, 54.

Jamiołkowski, A., 1972, Rep. Math. Phys. **3**, 275.

Jia, L., Z. Tian, and J. Jing, 2015, Ann. Phys. (Amsterdam) **353**, 37.

Julsgaard, B., J. Sherson, J. I. Cirac, J. Fiurášek, and E. S. Polzik, 2004, Nature (London) **432**, 482.

Kalev, A., and G. Gour, 2014, New J. Phys. **16**, 053038.

Kaniewski, J., M. Tomamichel, E. Hanggi, and S. Wehner, 2013, IEEE Trans. Inf. Theory **59**, 4687.

Kaniewski, J., M. Tomamichel, and S. Wehner, 2014, Phys. Rev. A **90**, 012332.

Karpat, G., J. Piilo, and S. Maniscalco, 2015, Europhys. Lett. **111**, 50006.

Kennard, E. H., 1927, Z. Phys. **44**, 326.

Kilian, J., 1988, in *Proceedings of ACM STOC 1988* (ACM Press, New York), pp. 20–31.
Klappenecker, A., and M. Rotteler, 2005, in *Proceedings of IEEE ISIT 2005* (IEEE, New York), pp. 1740–1744.
Koashi, M., 2006, J. Phys. Conf. Ser. **36**, 98.
König, R., and R. Renner, 2011, IEEE Trans. Inf. Theory **57**, 4760.
König, R., R. Renner, and C. Schaffner, 2009, IEEE Trans. Inf. Theory **55**, 4337.
König, R., S. Wehner, and J. Wullschleger, 2012, IEEE Trans. Inf. Theory **58**, 1962.
Korzekwa, K., D. Jennings, and T. Rudolph, 2014, Phys. Rev. A **89**, 052108.
Korzekwa, K., M. Lostaglio, D. Jennings, and T. Rudolph, 2014, Phys. Rev. A **89**, 042122.
Kraus, K., 1987, Phys. Rev. D **35**, 3070.
Krishna, M., and K. R. Parthasarathy, 2002, Indian Journal of Statistics **64**, 842 [http://www.jstor.org/stable/25051432].
Kuznetsova, A. A., 2011, Theory Probab. Appl. **55**, 709.
Larsen, U., 1990, J. Phys. A **23**, 1041.
Li, C.-F., J.-S. Xu, X.-Y. Xu, K. Li, and G.-C. Guo, 2011, Nat. Phys. **7**, 752.
Lieb, E. H., and M. B. Ruskai, 1973, J. Math. Phys. (N.Y.) **14**, 1938.
Lindblad, G., 1975, Commun. Math. Phys. **40**, 147.
Liu, S., L.-Z. Mu, and H. Fan, 2015, Phys. Rev. A **91**, 042133.
Liu, Y.-K., 2014, in *Proceedings of CRYPTO 2014*, LNCS, Vol. 8617, edited by J. A. Garay and R. Gennaro (Springer, Santa Barbara, CA), pp. 19–36.
Liu, Y.-K., 2015, in *Proceedings of EUROCRYPT 2015*, LNCS, Vol. 9057 (Springer, New York), pp. 785–814.
Lo, H.-k., 1997, Phys. Rev. A **56**, 1154.
Lo, H.-k., and H. F. Chau, 1997, Phys. Rev. Lett. **78**, 3410.
Luo, S. L., 2005, Theor. Math. Phys. **143**, 681.
Maassen, H., and J. Uffink, 1988, Phys. Rev. Lett. **60**, 1103.
Maccone, L., and A. K. Pati, 2014, Phys. Rev. Lett. **113**, 260401.
Mandayam, P., and S. Wehner, 2011, Phys. Rev. A **83**, 022329.
Mandayam, P., S. Wehner, and N. Balachandran, 2010, J. Math. Phys. (N.Y.) **51**, 082201.
Marshall, A. W., I. Olkin, and B. C. Arnold, 2011, *Inequalities: Theory of Majorization and Its Applications*, Springer Series in Statistics (Springer, New York).
Matthews, W., S. Wehner, and A. Winter, 2009, Commun. Math. Phys. **291**, 813.
Maurer, U. M., 1992, J. Cryptol. **5**, 53.
Mayers, D., 1996, in *Proceedings of CRYPTO 1996*, LNCS, Vol. 1109 (Springer, New York), pp. 343–357.
Mayers, D., 1997, Phys. Rev. Lett. **78**, 3414.
Mayers, D., 2001, J. Assoc. Comput. Mach. **48**, 351.
Mclnnes, J., 1987, Technical Report 194/87, Department of Computer Science, University of Toronto.
Miller, C. A., and Y. Shi, 2014, in *Proceedings of ACM STOC 2014* (ACM Press, New York), pp. 417–426.
Modi, K., A. Brodutch, H. Cable, T. Paterek, and V. Vedral, 2012, Rev. Mod. Phys. **84**, 1655.
Mosonyi, M., and T. Ogawa, 2015, Commun. Math. Phys. **334**, 1617.
Müller-Lennert, M., F. Dupuis, O. Szehr, S. Fehr, and M. Tomamichel, 2013, J. Math. Phys. (N.Y.) **54**, 122203.
Namiki, R., and Y. Tokunaga, 2012, Phys. Rev. Lett. **108**, 230503.
Narasimhachar, V., A. Poostindouz, and G. Gour, 2016, New J. Phys. **18**, 033019.
Ng, N. H. Y., M. Berta, and S. Wehner, 2012, Phys. Rev. A **86**, 042315.
Ohya, M., and D. Petz, 1993, *Quantum Entropy and Its Use* (Springer, New York).
Ollivier, H., and W. H. Zurek, 2001, Phys. Rev. Lett. **88**, 017901.
Oppenheim, J., and S. Wehner, 2010, Science **330**, 1072.
Ozawa, M., 2003, Phys. Rev. A **67**, 042105.
Partovi, M., 1983, Phys. Rev. Lett. **50**, 1883.
Partovi, M. H., 2011, Phys. Rev. A **84**, 052117.
Pati, A. K., M. M. Wilde, A. R. U. Devi, A. K. Rajagopal, and Sudha, 2012, Phys. Rev. A **86**, 042105.
Prevedel, R., D. R. Hamel, R. Colbeck, K. Fisher, and K. J. Resch, 2011, Nat. Phys. **7**, 757.
Puchała, Z., Ł. Rudnicki, K. Chabuda, M. Paraniak, and K. Życzkowski, 2015, Phys. Rev. A **92**, 032109.
Puchała, Z., Ł. Rudnicki, and K. Życzkowski, 2013, J. Phys. A **46**, 272002.
Rastegin, A. E., 2013a, Quantum Inf. Process. **12**, 2947.
Rastegin, A. E., 2013b, Eur. Phys. J. D **67**, 269.
Rastegin, A. E., 2014, Commun. Theor. Phys. **61**, 293.
Rastegin, A. E., 2015a, Quantum Inf. Process. **14**, 783.
Rastegin, A. E., 2015b, Open Syst. Inf. Dyn. **22**, 1550005.
Rastegin, A. E., 2015c, Found. Phys. **45**, 923.
Rastegin, A. E., and K. Życzkowski, 2016, J. Phys. A **49**, 355301.
Ren, L.-H., and H. Fan, 2014, Phys. Rev. A **90**, 052110.
Renes, J., and J.-C. Boileau, 2009, Phys. Rev. Lett. **103**, 020402.
Renes, J. M., R. Blume-Kohout, A. J. Scott, and C. M. Caves, 2004, J. Math. Phys. (N.Y.) **45**, 2171.
Renes, J. M., and J.-C. Boileau, 2008, Phys. Rev. A **78**, 032335.
Renes, J. M., D. Sutter, F. Dupuis, and R. Renner, 2015, IEEE Trans. Inf. Theory **61**, 6395.
Renes, J. M., and M. M. Wilde, 2014, IEEE Trans. Inf. Theory **60**, 3090.
Renner, R., 2005, Security of Quantum Key Distribution, Ph.D. thesis (ETH, Zurich).
Renner, R., and R. König, 2005, in *Proceedings of TCC 2005*, LNCS, Vol. 3378 (Springer, Berlin), pp. 407–425.
Rényi, A., 1961, in *Proceedings of the 4th Berkeley Symposium on Mathematical Statistics and Probability*, Vol. 1 (University of California Press, Berkeley, CA), pp. 547–561.
Robertson, H. P., 1929, Phys. Rev. **34**, 163.
Rojas González, A., J. A. Vaccaro, and S. M. Barnett, 1995, Phys. Lett. A **205**, 247.
Romera, E., and M. Calixto, 2015, J. Phys. Condens. Matter **27**, 175003.
Rudnicki, Ł., 2011, J. Russ. Laser Res. **32**, 393.
Rudnicki, Ł., 2015, Phys. Rev. A **91**, 032123.
Rudnicki, Ł., Z. Puchała, and K. Życzkowski, 2014, Phys. Rev. A **89**, 052115.
Rudnicki, Ł., S. P. Walborn, and F. Toscano, 2012, Phys. Rev. A **85**, 042115.
Rumin, M., 2011, Duke Math. J. **160**, 567.
Rumin, M., 2012, Lett. Math. Phys. **100**, 291.
Saboia, A., F. Toscano, and S. P. Walborn, 2011, Phys. Rev. A **83**, 032307.
Sánchez-Ruiz, J., 1993, Phys. Lett. A **173**, 233.
Sánchez-Ruiz, J., 1995, Phys. Lett. A **201**, 125.
Sánchez-Ruiz, J., 1998, Phys. Lett. A **244**, 189.
Scarani, V., H. Bechmann-Pasquinucci, N. Cerf, M. Dusek, N. Lütkenhaus, and M. Peev, 2009, Rev. Mod. Phys. **81**, 1301.
Schaffner, C., 2007, "Cryptography in the Bounded-Quantum-Storage Model," Ph.D thesis (University of Aarhus).
Schneeloch, J., C. J. Broadbent, and J. C. Howell, 2014, Phys. Rev. A **90**, 062119.
Schneeloch, J., C. J. Broadbent, S. P. Walborn, E. G. Cavalcanti, and J. C. Howell, 2013, Phys. Rev. A **87**, 062103.

Schrödinger, E., 1930, *Proceedings of the Prussian Academy of Sciences* XIX, 296.
Schrödinger, E., 1935, Math. Proc. Cambridge Philos. Soc. **31**, 555.
Schumacher, B., and M. A. Nielsen, 1996, Phys. Rev. A **54**, 2629.
Shannon, C., 1948, Bell Syst. Tech. J. **27**, 379.
Shor, P. W., and J. Preskill, 2000, Phys. Rev. Lett. **85**, 441.
Slepian, D., and H. O. Pollak, 1961, Bell Syst. Tech. J. **40**, 43.
Stinespring, W. F., 1955, Proc. Am. Math. Soc. **6**, 211 [http://www.ams.org/journals/proc/1955-006-02/S0002-9939-1955-0069403-4/home.html].
Tomamichel, M., 2012, A Framework for Non-Asymptotic Quantum Information Theory, Ph.D. thesis (ETH Zurich).
Tomamichel, M., 2016, *Quantum Information Processing with Finite Resources—Mathematical Foundations*, Springer Briefs in Mathematical Physics, Vol. 5 (Springer International Publishing, Heidelberg).
Tomamichel, M., M. Berta, and M. Hayashi, 2014, J. Math. Phys. (N.Y.) **55**, 082206.
Tomamichel, M., R. Colbeck, and R. Renner, 2009, IEEE Trans. Inf. Theory **55**, 5840.
Tomamichel, M., R. Colbeck, and R. Renner, 2010, IEEE Trans. Inf. Theory **56**, 4674.
Tomamichel, M., S. Fehr, J. Kaniewski, and S. Wehner, 2013, New J. Phys. **15**, 103002.
Tomamichel, M., and E. Hänggi, 2013, J. Phys. A **46**, 055301.
Tomamichel, M., C. C. W. Lim, N. Gisin, and R. Renner, 2012, Nat. Commun. **3**, 634.
Tomamichel, M., and R. Renner, 2011, Phys. Rev. Lett. **106**, 110506.
Tomamichel, M., C. Schaffner, A. Smith, and R. Renner, 2011, IEEE Trans. Inf. Theory **57**, 5524.
Tsallis, C., 1988, J. Stat. Phys. **52**, 479.
Uffink, J., 1990, Measures of Uncertainty and the Uncertainty Principle, Ph.D. thesis (R. U. Utrecht).
Uhlmann, A., 1977, Commun. Math. Phys. **54**, 21.
Uhlmann, A., 1985, Ann. Phys. (N.Y.) **497**, 524.
Umegaki, H., 1962, Kodai Math. Sem. Rep. **14**, 59.
Unruh, D., 2010, in *Proceedings of EUROCRYPT 2010*, LNCS, Vol. 6110 (Springer, New York), pp. 486–505.
Vaccaro, J. A., 2011, Proc. R. Soc. A **468**, 1065.
Vadhan, S. P., 2012, Foundations and Trends in Theoretical Computer Science **7**, 1.
Vallone, G., D. G. Marangon, M. Tomasin, and P. Villoresi, 2014, Phys. Rev. A **90**, 052327.
Ver Steeg, G., and S. Wehner, 2009, Quantum Inf. Comput. **9**, 0801 [http://www.rintonpress.com/journals/qiconline.html#v9n910].
von Neumann, J., 1932, *Mathematische Grundlagen der Quantenmechanik* (Springer, New York).
Walborn, S. P., A. Salles, R. M. Gomes, F. Toscano, and P. H. Souto Ribeiro, 2011, Phys. Rev. Lett. **106**, 130402.
Walborn, S. P., B. G. Taketani, A. Salles, F. Toscano, and R. L. de Matos Filho, 2009, Phys. Rev. Lett. **103**, 160505.
Weedbrook, C., S. Pirandola, R. García-Patrón, N. Cerf, T. Ralph, J. Shapiro, and S. Lloyd, 2012, Rev. Mod. Phys. **84**, 621.
Wehner, S., C. Schaffner, and B. M. Terhal, 2008, Phys. Rev. Lett. **100**, 220502.
Wehner, S., and A. Winter, 2008, J. Math. Phys. (N.Y.) **49**, 062105.
Wehner, S., and A. Winter, 2010, New J. Phys. **12**, 025009.
Wehrl, A., 1978, Rev. Mod. Phys. **50**, 221.
Weyl, H., 1928, *Gruppentheorie und Quantenmechanik* (Hirzel, Leipzig).
Wilde, M. M., A. Winter, and D. Yang, 2014, Commun. Math. Phys. **331**, 593.
Winter, A., and D. Yang, 2016, Phys. Rev. Lett. **116**, 120404.
Wiseman, H. M., S. J. Jones, and A. C. Doherty, 2007, Phys. Rev. Lett. **98**, 140402.
Wootters, W., and W. H. Zurek, 1979, Phys. Rev. D **19**, 473.
Wootters, W. K., and B. D. Fields, 1989, Ann. Phys. (N.Y.) **191**, 363.
Wootters, W. K., and D. M. Sussman, 2007, in *Proceedings of QCMC 2007*, p. 269, arXiv:0704.1277.
Wootters, W. K., and W. H. Zurek, 1982, Nature (London) **299**, 802.
Wu, S., S. Yu, and K. Molmer, 2009, Phys. Rev. A **79**, 022104.
Zozor, S., G. M. Bosyk, and M. Portesi, 2013, J. Phys. A **46**, 465301.
Zozor, S., G. M. Bosyk, and M. Portesi, 2014, J. Phys. A **47**, 495302.
Zurek, W. H., 2003, Rev. Mod. Phys. **75**, 715.
Życzkowski, K., and I. Bengtsson, 2004, Open Syst. Inf. Dyn. **11**, 3.