

# The Link between Entropic Uncertainty and Nonlocality

Marco Tomamichel<sup>1,2,\*</sup> and Esther Hänggi<sup>1</sup>

<sup>1</sup>*Centre for Quantum Technologies, National University of Singapore, Singapore*

<sup>2</sup>*Institute for Theoretical Physics, ETH Zurich, 8093 Zurich, Switzerland*

Two of the most intriguing features of quantum physics are the *uncertainty principle* and the occurrence of *nonlocal correlations*. The uncertainty principle states that there exist pairs of incompatible measurements on quantum systems such that their outcomes cannot both be predicted. On the other hand, nonlocal correlations of measurement outcomes at different locations cannot be explained by classical physics, but appear in the presence of entanglement. Here, we show that these two fundamental quantum effects are quantitatively related. Namely, we provide an entropic uncertainty relation for the outcomes of two binary measurements, where the lower bound on the uncertainty is quantified in terms of the maximum Clauser-Horne-Shimony-Holt value that can be achieved with these measurements. We discuss applications of this uncertainty relation in quantum cryptography, in particular, to certify quantum sources using untrusted devices.

## I. INTRODUCTION

A remarkable characteristic of quantum physics is the *uncertainty principle*, as first described by Heisenberg [21] and Robertson [44]. It expresses the fact that there exist certain observable properties of a quantum system such that knowledge of one necessarily implies uncertainty about the other. In recent relations, starting with [15, 31], the uncertainty of a measurement is often quantified in terms of entropies evaluated for the probability distribution over measurement outcomes induced by Born’s rule. Roughly speaking, if the distribution over the different measurement outcomes is close to uniform, the entropy is large and the uncertainty high; on the other hand, a peaked distribution leads to small entropy and low uncertainty. An entropic uncertainty relation provides a lower bound on the sum of the entropies of two or more alternative measurements that is valid for all states of the quantum system prior to measurement. This bound is trivial for compatible measurements and can generally be seen as a measure of “incompatibility” of the measurements. We restrict the discussion to measurements with a finite number of different outcomes hereafter, and point to a recent review of the topic by Wehner and Winter [58].

A prominent example of such an uncertainty relation is the one shown by Maassen and Uffink [31]. It states that the Shannon entropy of the outcomes of two non-degenerate measurements,  $X$  and  $Y$ , is lower bounded by a function of their *overlap*,  $c$ . Namely,

$$H(X) + H(Y) \geq -\log_2 c, \quad \text{where} \quad c = \max_{i,j} |\langle \phi^i | \psi^j \rangle|^2. \quad (1)$$

The overlap of the two measurements is a function of their eigenvectors,  $|\phi^i\rangle$  and  $|\psi^j\rangle$ , respectively. (We shall make this statement more formal in the following sections.)

In [5, 9, 10, 52], entropic uncertainty relations have been extended to include the case where observers have access to a quantum memory, i.e. a quantum system that is correlated with the state prior to measurement. Note that an entangled observer can in principle perfectly predict the outcomes of both measurements appearing in Eq. (1) by applying an appropriate measurement on his memory. Thus, Eq. (1) is no longer valid when the Shannon entropies are replaced by von Neumann entropies conditioned on the observers memory. (We refer to the discussion in [5] for

---

\* [cqtmarco@nus.edu.sg](mailto:cqtmarco@nus.edu.sg)

more details.) This limitation can be overcome by introducing tripartite uncertainty relations, where one considers two separate quantum memories,  $B$  (controlled by Bob) and  $C$  (controlled by Charlie) and takes advantage of the monogamy of entanglement. Surprisingly, uncertainty relations of a similar form as (1) result, but now the uncertainty is formulated in terms of conditional von Neumann entropies and reads [5]

$$H(X|B) + H(Y|C) \geq -\log_2 c. \quad (2)$$

This inequality can be interpreted as follows. If Bob can predict the outcome of the  $X$  measurement with certainty (i.e.,  $H(X|B) = 0$ ), then Charlie necessarily has uncertainty about the outcome of the  $Y$  measurement (i.e.,  $H(Y|C) > 0$ ) as long as the measurements are incompatible (i.e.,  $c < 1$ ). Note also that (2) implies (1) due to the strong sub-additivity of the von Neumann entropy [29] and is, therefore, strictly stronger.

In the context of cryptography, uncertainty of an eavesdropper implies (partial) secrecy, and indeed entropic uncertainty relations have been employed to show cryptographic security [12, 13, 25, 51, 52]. More generally, the usefulness of these uncertainty relations can be understood from the fact that the entropies on the lefthand side of (1) and (2) characterize operational quantities in information theory, e.g. the asymptotic data compression rate [16, 46].

Another phenomenon distinguishing quantum from classical physics is the occurrence of *nonlocal correlations*. It has already been observed by Einstein, Podolsky and Rosen [18] that quantum mechanics predicts correlations between entangled, but spatially separated particles, which are stronger than one would intuitively expect. Bell [2] later showed that these correlations cannot be explained by any classical local theory; hence, they are called nonlocal.

Nonlocality can be quantified using so-called Bell inequalities [2]. A prominent example is the Clauser-Horne-Shimony-Holt (CHSH) inequality [7], which considers a bipartite setup where two separated parties, called Alice ( $A$ ) and David ( $D$ ), share a potentially entangled quantum state. Both parties randomly choose one out of two binary measurements that they apply to their share of the quantum state. We denote the outcomes of Alice's measurements by the random variables  $X$  and  $Y$  (as in the setup of the uncertainty relation) and David's outcomes by  $R$  and  $S$ , depending on his choice of measurement. The CHSH inequality states that, for any classically correlated state, it holds that  $\beta \leq 2$ , where

$$\beta = 2\Pr[X = R] + 2\Pr[Y = R] + 2\Pr[X = S] + 2\Pr[Y \neq S] - 4 \quad (3)$$

is called the *CHSH value*. If  $\beta > 2$ , we call the correlation nonlocal, and quantum mechanics allows correlations that achieve up to  $\beta_{\max} = 2\sqrt{2}$ , which is called Tsirelson's bound [54]. (Nonlocal correlations can, for example, be realized using an entangled pair of spin-1/2 particles, where the choice of measurement corresponds to a spin direction. However, we will not make any assumption about how the system is physically realized in the following.)

The remainder of this paper is structured as follows. Section II discusses related work. Section III states the main results of our work, which provide a link between entropic uncertainty and nonlocality. Finally, Section IV sketches an application of our results to self-testing sources of Bennett-Brassard 84 states. The formal proofs of the main results are deferred to the appendix.

## II. RELATED WORK

The main result of this paper is a quantitative relation between entropic uncertainty and nonlocality. The fact that the incompatibility of local measurements and nonlocality are related in some way is folklore knowledge and follows, for example, from the work of Tsirelson [54]. For the

case when the systems are restricted to qubits, a bound on the maximal CHSH value in terms of the angle between local measurements has been derived by Seevinck and Uffink [45]. The analytical form of Relation (5) has been conjectured by Horodecki [22] and derived independently by Lim [30] for the case of single qubit systems. Mayers and Yao have shown that in order to reach the maximal CHSH value allowed by quantum physics, the state and measurements essentially need to be (equivalent to) a fully entangled state and optimal CHSH measurements even when they are embedded in higher dimensions [35, 36]. They also employed this result in quantum cryptography, where they used it to construct self-testing sources.

We improve these results by providing an exact analytical relation that characterizes all allowed combinations of local overlap and CHSH value. In particular, our result is independent of the system dimension and the quantum state under consideration. Furthermore, the overlap—in contrast to other measures of incompatibility based on the commutator of the observables or the angle between measurements that have been investigated previously—attains operational meaning in quantum information theory through the entropic uncertainty relations. Following Mayers and Yao, we also sketch an application our result to self-testing sources.

On a related topic, Oppenheim and Wehner [39]—for a class of generalized physical theories that includes quantum mechanics and classical theory—showed that the presence of uncertainty, via steering, directly limits the maximally achievable nonlocality. Our result can be seen as complementary to theirs, as we show that in order to achieve a certain nonlocality, at least some specific amount of uncertainty is necessary.

Device-independent quantum key distribution [1, 20, 32, 34, 37] and randomness generation [8] usually bases security on a relation between nonlocality and the randomness of the outcomes relative to some (quantum) adversary. Our result allows to split the security analysis of these protocols into two parts: the nonlocality of the measured correlations first gives a bound on the uncertainty of local measurement outcomes, which in turn can be used to ensure security. The two parts can be analyzed independently and thus our methods can be used to simplify such an analysis and, potentially, reduce the required assumptions.

### III. MAIN RESULTS

In order to present our main results, we employ the density operator formalism of quantum mechanics in finite dimensions and use standard notation that we quickly summarize here.

#### A. Notation

A *quantum state* is represented by a positive semidefinite operator with unit trace acting on a finite-dimensional Hilbert space. We consider states shared between different locations, which are described as operators acting on the tensor product of the respective local spaces. For example, we denote by  $\rho_{AB}$  a state shared between locations  $A$  and  $B$  and by  $\rho_B = \text{tr}_A(\rho_{AB})$  its marginal state on  $B$ , where  $\text{tr}_A$  is the partial trace over  $A$ .

A quantum measurement can be most generally described by a *positive operator-valued measure* (POVM). The measure induces a *completely positive trace-preserving map* (CPTPM) that maps states on  $A$  to a classical register that contains the measurement outcome. Within the quantum formalism, a classical register (or random variable) is described by a Hilbert space with a fixed basis and states that are diagonal in this basis. For example, let  $\mathbf{X} = \{M_A^x\}$  be a measurement with discrete outcomes on  $A$ , i.e. a set indexed by  $x$  of positive semidefinite operators  $M_A^x$  on  $A$  satisfying  $\sum_x M_A^x = \mathbb{1}_A$ , where  $\mathbb{1}_A$  is the identity operator on  $A$ . The corresponding measurement

map,  $\mathcal{M}_X$  from  $A$  to the register  $X$ , thus produces states of the form

$$\mathcal{M}_X : \rho_{AB} \mapsto \rho_{XB} = \sum_x |x\rangle\langle x|_X \otimes \text{tr}_A((M_A^x \otimes \mathbb{1}_B)\rho_{AB}) = \sum_x p_x |x\rangle\langle x|_X \otimes \rho_B^x,$$

where  $p_x = \text{tr}(M_A^x \rho_A)$  is the probability with which outcome  $x$  occurs,  $\rho_B^x = \frac{1}{p_x} \text{tr}_A(M_A^x \rho_{AB})$  is the state of  $B$  conditioned on the event that  $x$  was measured and  $|x\rangle\langle x|_X$  is the projector onto an element of a fixed orthonormal basis  $\{|x\rangle\}$  of  $X$ . (Note that we often omit writing the identity operator when it is clearly implied by context.) We call a measurement *projective* if the operators  $M_A^x$  are projectors, i.e. if  $M_A^x M_A^x = M_A^x$  for all  $x$ .

We also use the fact that non-projective measurements can be seen as projective measurements of an enlarged quantum system. More precisely, a *dilation* of a measurement  $X = \{M_A^x\}$  consists of an embedding  $U : A \rightarrow A'$  that embeds  $A$  into a larger space  $A'$  and a measurement  $X' = \{M_{A'}^x\}$  on  $A'$  such that  $U^\dagger M_{A'}^x U = M_A^x$  for all  $x$ . The latter condition ensures that, for every state  $\rho_{AB}$ , we have  $\rho_{XB} = \mathcal{M}_X[\rho_{AB}] = \mathcal{M}_{X'}[U\rho_{AB}U^\dagger]$ , i.e. the post measurement states of the two measurements are equal. Moreover, Neumark's dilation theorem [38] ensures that if  $A'$  is chosen sufficiently large, there always exists a dilation such that  $X'$  is projective.

We employ the operator norm  $\|\cdot\|$ , which evaluates to the largest eigenvalue for Hermitian operators. Moreover, we define the conditional von Neumann entropy,  $H(A|B)_\rho := H(AB)_\rho - H(B)_\rho$ , where  $H(A)_\rho := -\text{tr}(\rho_A \log_2 \rho_A)$ . Note that for the above example  $H(X)_\rho$  reduces to the Shannon entropy of the probability distribution  $p_x$  induced by the measurement and that  $H(X|B)_\rho \leq H(X)_\rho$  due to the strong sub-additivity of the von Neumann entropy [29].

This formalism allows us to restate the uncertainty relation (2) in its full generality [9, 28, 52]. Given any tripartite quantum state  $\rho_{ABC}$  and two measurements  $X = \{M_A^x\}$  and  $Y = \{N_A^y\}$  on  $A$ , the post measurement states  $\rho_{XB} = \mathcal{M}_X[\rho_{AB}]$  and  $\rho_{YC} = \mathcal{M}_Y[\rho_{AC}]$  satisfy

$$H(X|B)_\rho + H(Y|C)_\rho \geq -\log_2 c(X, Y), \quad \text{where} \quad c(X, Y) := \max_{x, y} \left\| \sqrt{M_A^x} N_A^y \sqrt{M_A^x} \right\|. \quad (4)$$

This relation gives a bound on the uncertainty in terms of the overlap which is a function of the two measurements but independent of the quantum state of the system prior to measurement. Note that  $c(X, Y)$  reduces to the expression in (1) in the case of non-degenerate projective measurements.

## B. Generalized Uncertainty Relations

While the overlap, and thus the uncertainty, can be calculated from the POVM elements associated with the two measurements alone, it cannot be tested experimentally. Hence, in practice, determining the uncertainty a measurement produces requires a precise theoretical model of the measurement devices used and any deviation of the physical implementation from this theoretical model may lead to an overestimation of the produced uncertainty. Specifically, this is of critical importance in quantum cryptography, where uncertainty of one observer ensures security for the others, and an overestimation of this uncertainty directly leads to a security loophole.

In this work, we will thus introduce a variation of the overlap, the *effective overlap*, which can be tested experimentally in an important special case as we will see below. The definition of the effective overlap is motivated by the following two observations.

- The entropies on the left-hand side of the uncertainty relation (4) are evaluated for the post measurement states  $\rho_{XB}$  and  $\rho_{YC}$  that result from measuring  $X$  and  $Y$  on  $\rho_{ABC}$ , respectively. However, these post measurement states can generally also be constructed in other ways and it is evident that the right-hand side of (4) can thus be maximized over all pairs

of measurements that achieve the post measurement states  $\rho_{XB}$  and  $\rho_{YC}$ . A generic construction of such measurements is given by any pair of joint dilations  $\{U, X'\}$  and  $\{U, Y'\}$  of  $X$  and  $Y$  based on the same embedding  $U : A \rightarrow A'$ . The post measurement states can now alternatively be constructed as  $\rho_{XB} = \mathcal{M}_{X'}[U\rho_{AB}U^\dagger]$  and  $\rho_{YC} = \mathcal{M}_{Y'}[U\rho_{AC}U^\dagger]$  and the right-hand side of (4) can be evaluated either for  $c(X, Y)$  or for  $c(X', Y')$ .

- Moreover, any projective measurement on  $A$ —let us denote it by  $K = \{P_A^k\}$ —can be used to slice the state into orthogonal parts before the actual measurements are applied. This results in an intermediate state of the form  $\sum_k P_A^k \rho_{ABC} P_A^k$ . Moreover, if this extra measurement commutes with both  $X$  and  $Y$  on the support of  $\rho_A$ , the respective post measurement states with and without slicing are indistinguishable, i.e. we have  $\rho_{XB} = \mathcal{M}_X[\rho_{AB}] = \mathcal{M}_X[\sum_k P_A^k \rho_{AB} P_A^k]$  and  $\rho_{YC} = \mathcal{M}_Y[\rho_{AC}] = \mathcal{M}_Y[\sum_k P_A^k \rho_{AC} P_A^k]$ . We will see in the following that the overlap of the measurements  $X$  and  $Y$  on the sliced state is given by the average overlap evaluated for the individual slices.

We combine these two observations to define the *effective overlap* as a function of a *measurement setup*, which consists of two measurements and the marginal state  $\rho_A$  on  $A$  that will be measured.

*Definition 1.* Let  $\rho_A$  be a quantum state and let  $X = \{M_A^x\}$  and  $Y = \{N_A^y\}$  be two measurements on  $A$ . The effective overlap of the measurement setup  $\{\rho_A, X, Y\}$  is defined as

$$c^*(\rho_A, X, Y) := \inf_{U, X', Y', K'} \left\{ \sum_k \text{tr}(P_{A'}^k U \rho_A U^\dagger) \max_x \left\| \sum_y P_{A'}^k N_{A'}^y P_{A'}^k \cdot P_{A'}^k M_{A'}^x P_{A'}^k \cdot P_{A'}^k N_{A'}^y P_{A'}^k \right\| \right\}$$

where the infimum is taken over all embeddings  $U$  from  $A$  to an auxiliary space  $A'$ , all measurements  $X' = \{M_{A'}^x\}$  and  $Y' = \{N_{A'}^y\}$  on  $A'$ , and all projective measurements  $K' = \{P_{A'}^k\}$  on  $A'$  such that  $\sum_k U^\dagger P_{A'}^k M_{A'}^x P_{A'}^k U = M_A^x$  and  $\sum_k U^\dagger P_{A'}^k N_{A'}^y P_{A'}^k U = N_A^y$  for all  $x$  and  $y$ .

Note that while evaluating the effective overlap for a general measurement setup might be intractable, it is often easy to find upper bounds on it. To see this, consider the following example, where the effective overlap leads to a tighter characterization of the uncertainty.

We apply one of two projective measurements, either in the basis  $\{|0\rangle, |1\rangle, |\perp\rangle\}$  or in the basis  $\{|+\rangle, |-\rangle, |\perp\rangle\}$ , where  $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$ . These measurements are applied on a state  $\rho$  which has the property that ‘ $\perp$ ’ is measured with probability at most  $\varepsilon$ . The uncertainty relation (4) gives a trivial bound as the overlap of the two bases is  $c = 1$ . Still, our intuitive understanding is that the uncertainty about the measurement outcome is high as long as  $\varepsilon$  is small. In fact, it is easy to verify that the effective overlap of this setup satisfies  $c^* \leq (1 - \varepsilon)\frac{1}{2} + \varepsilon$  and thus captures this intuition. (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  $\frac{1}{2}$ , and with probability  $\varepsilon$  we measure  $\perp$  and have maximal overlap.)

Our first result is a generalization of the uncertainty relations (1) and (2). We show that these relations still hold when the overlap is replaced by the effective overlap.

**Theorem 1.** *Let  $\rho_{ABC}$  be a tripartite quantum state and  $X = \{M_A^x\}$  and  $Y = \{N_A^y\}$  two measurements on  $A$ . Then, the states  $\rho_{XB} = \mathcal{M}_X[\rho_{AB}]$  and  $\rho_{YC} = \mathcal{M}_Y[\rho_{AC}]$  satisfy*

$$H(X)_\rho + H(Y)_\rho \geq H(X|B)_\rho + H(Y|C)_\rho \geq -\log_2 c^*(\rho_A, X, Y).$$

The proof of this theorem employs the *smooth entropy framework* [43, 48, 50], which has already found many applications in quantum cryptography and non-asymptotic information theory. In the process, we also generalize an entropic uncertainty relation for smooth entropies [52].

Let us thus explain in more detail why an uncertainty relation in terms of smooth min- and max-entropy is desirable. The von Neumann entropy used above (and its classical analogue, the Shannon entropy) characterizes information theoretic tasks in the asymptotic limit of many independent repetitions. In practice, one can neither perform an infinite number of repetitions of an experiment, nor are the different runs usually independent of each other. In the setting where we would like to characterize the resources related to a task which is repeated only once, called the *one-shot* setting, the smooth min- and max-entropies often take the role of von Neumann entropy. In order for them to be applicable to the analysis of realistic protocols it is therefore crucial to develop uncertainty relations in terms of smooth entropies.

The smooth entropies can be interpreted as operational quantities in the following sense. On the one hand, the smooth min-entropy,  $H_{\min}^{\varepsilon}(X|B)$ , quantifies the maximal number of uniformly random bits, independent of quantum side information  $B$ , that can be extracted from  $X$  [43, 53]. This quantity is of particular importance in cryptography, where the task often involves extracting randomness that is secret from a quantum adversary. On the other hand, the smooth max-entropy,  $H_{\max}^{\varepsilon}(Y|C)$ , quantifies the minimum number of additional bits of information about  $Y$  that are needed to reconstruct  $Y$  from a quantum memory  $C$  [42]. In both cases, the *smoothing parameter*,  $\varepsilon$ , ensures the quality of the resulting state, i.e. it has to be indistinguishable from a perfect output up to probability  $\varepsilon$ .

The following relation is thus of independent interest and shows that the uncertainty relation for smooth entropies in [52] also holds for the effective overlap.

**Theorem 2.** *Let  $\rho_{ABC}$  be a tripartite quantum state,  $\varepsilon \geq 0$ ,  $\bar{\varepsilon} > 0$  and let  $\mathbf{X} = \{M_A^x\}$  and  $\mathbf{Y} = \{N_A^y\}$  two POVMs on  $A$ . Then, the states  $\rho_{XB} = \mathcal{M}_{\mathbf{X}}[\rho_{AB}]$  and  $\rho_{YC} = \mathcal{M}_{\mathbf{Y}}[\rho_{AC}]$  and the smooth min- and max-entropies as defined in Appendix A satisfy*

$$H_{\min}^{\varepsilon+2\bar{\varepsilon}}(X|B)_{\rho} + H_{\max}^{\varepsilon}(Y|C)_{\rho} \geq -\log_2 c^*(\rho_A, \mathbf{X}, \mathbf{Y}) - \log_2(2/\bar{\varepsilon}^2).$$

The relation in the above form directly leads to a formal security proof of quantum key distribution (QKD) against general adversaries while at the same time making it more robust against device imperfections, in analogy with [51, 52]. To see how this works, consider the entanglement based version of the Bennett-Brassard 1984 protocol [3, 4] and  $n$  measurements in the computational and diagonal basis such that  $-\log_2 c^* = n$ . The uncertainty relation is now applied to the situation where Alice and Bob would like to agree on a key, while Charlie takes the role of the eavesdropper. Using the operational meaning of the smooth entropies as described above, the uncertainty relation states that the number of secret bits extractable from a raw string  $Y^n$  is given by  $n$  minus the number of additional bits from Alice required for Bob to correct phase errors (i.e. the errors in  $X^n$ ). The latter number, however, can be inferred by Alice and Bob from experimental data, and thus the security of the extracted key can be ensured by them without making any assumptions about the eavesdropper's attack.

The detailed proofs of Theorem 1 and 2 can be found in Appendix A.

### C. Relation between Overlap and Nonlocality

We now consider four POVM measurements with *binary* outcomes,  $\mathbf{X}$  and  $\mathbf{Y}$  on Alice's side as well as  $\mathbf{R}$  and  $\mathbf{S}$  on David's side. We first define the *CHSH value* of a *bipartite measurement setup*.

*Definition 2.* Let  $\rho_{AD}$  be a bipartite state and let  $\mathbf{X} = \{M_A^0, M_A^1\}$ ,  $\mathbf{Y} = \{N_A^0, N_A^1\}$  be measurements on  $A$  and  $\mathbf{R} = \{R_D^0, R_D^1\}$ ,  $\mathbf{S} = \{S_D^0, S_D^1\}$  be measurements on  $D$ . Then, the CHSH value of the



bipartite measurement setup  $\{\rho_{AD}, \mathbf{X}, \mathbf{Y}, \mathbf{R}, \mathbf{S}\}$  is defined as

$$\beta(\rho_{AD}, \mathbf{X}, \mathbf{Y}, \mathbf{R}, \mathbf{S}) := 2 \operatorname{tr} \left( \sum_{i=0}^1 (M_A^i \otimes (R_D^i + S_D^i) + N_A^i \otimes (R_D^i + S_D^{1-i})) \rho_{AD} \right) - 4.$$

Note that the trace term corresponds to  $\Pr[X = R] + \Pr[Y = R] + \Pr[X = S] + \Pr[Y \neq S]$  in (3) evaluated for the state  $\rho_{AD}$  and the four specified POVMs.

The main result of this paper shows a relation between the effective overlap of Alice's measurement setup and  $\beta$ , the maximal CHSH value that can be reached between Alice and an arbitrary additional party, David, with the same measurement setup on Alice's side. (Alice's measurement setup is given by the marginal state on  $A$  as well as the two possible POVMs she can choose from.)

**Theorem 3.** *Let  $\rho_A$  be a state and let  $\mathbf{X}, \mathbf{Y}$  be binary measurements such that  $c^* = c^*(\rho_A, \mathbf{X}, \mathbf{Y})$ . Then, for any  $\rho_{AD}$  with  $\operatorname{tr}_D(\rho_{AD}) = \rho_A$  and any two binary measurements  $\mathbf{R}, \mathbf{S}$  on  $D$ , we have*

$$\beta(\rho_{AD}, \mathbf{X}, \mathbf{Y}, \mathbf{R}, \mathbf{S}) \leq 2(\sqrt{c^*} + \sqrt{1 - c^*}). \quad (5)$$

Conversely, for any bipartite state  $\rho_{AD}$  and any binary measurements  $\mathbf{X}, \mathbf{Y}$  on  $A$  and  $\mathbf{R}, \mathbf{S}$  on  $D$  such that  $\beta = \beta(\rho_{AD}, \mathbf{X}, \mathbf{Y}, \mathbf{R}, \mathbf{S})$ , we have

$$c^*(\rho_A, \mathbf{X}, \mathbf{Y}) \leq \frac{1}{2} + \frac{\beta}{8} \sqrt{8 - \beta^2}. \quad (6)$$

This bound is depicted in Figure 1 and implies as a special case that any state and measurement on Alice's part which can give rise to nonlocal correlations (i.e.,  $\beta > 2$ ), must have effective overlap  $c^* < 1$ . Furthermore, in order to reach a CHSH value close to Tsirelson's bound (i.e.,  $\beta \approx 2\sqrt{2}$ ), the measurement on  $A$  must have almost minimal overlap  $c^* \approx 1/2$ .

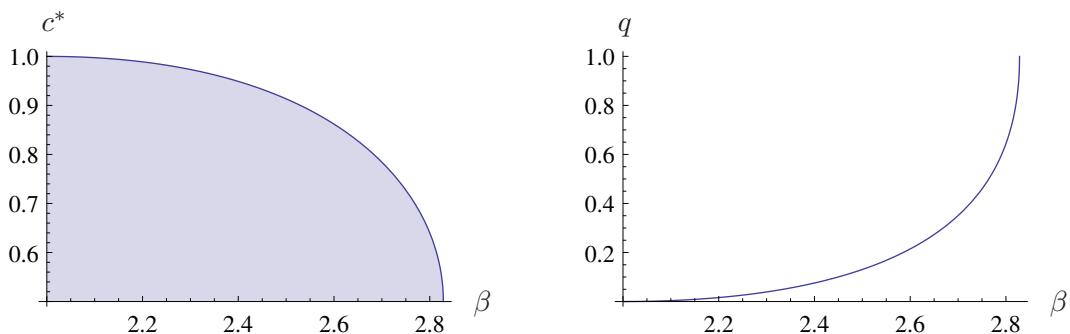


FIG. 1. The relation between local overlap and CHSH value. Due to our bound (6), combinations of  $\beta$  and  $c^*$  outside the filled region in the left figure are impossible. The right figure shows the guaranteed uncertainty,  $q = -\log_2 c^*$ , as a function of  $\beta$ .

Theorem 3 in particular implies that if Alice and David can experimentally verify that the CHSH violation of their bipartite setup exceeds some fixed value  $\beta$ , then the effective overlap of both Alice's and David's local measurements is upper bounded by (6).

Finally, Equation (6), together with Theorem 1, directly implies an uncertainty relation with quantum side information where the lower bound is stated in terms of the CHSH value the measurement setup can reach. This *device-independent uncertainty relation* is stated only in terms of quantities which have an operational meaning. We have

$$H(X)_\rho + H(Y)_\rho \geq H(X|B)_\rho + H(Y|C)_\rho \geq 1 - \log_2 \left( 1 + \frac{\beta}{4} \sqrt{8 - \beta^2} \right),$$

where  $\beta$  is the CHSH value between  $A$  and  $D$ , resulting from measuring any state  $\rho_{AD}$  with  $\text{tr}_T(\rho_{AD}) = \rho_A$  using measurements  $X$  and  $Y$  on  $A$  and arbitrary measurements on  $D$ . The right-hand side of this inequality, i.e. the guaranteed uncertainty, is also depicted in Figure 1.

This implies, for example, that if Bob’s uncertainty about Alice’s outcome is low, but the CHSH value between Alice and Bob (who takes the role of David in this example) is high, then Charlie’s uncertainty about the outcome of the other measurement must necessarily be high. Alice and Bob can therefore infer whether Charlie has high entropy from their correlations alone.

We want to stress again that previous uncertainty relations were stated in terms of the overlap, which can only be determined if the exact specification of Alice’s measurement devices is known. Our uncertainty relation, on the other hand, depends *only* on the observable quantity  $\beta$  and is independent of the details of the theoretical model used to describe the quantum systems and measurements. This includes, in particular, the dimension of the Hilbert space they act on.

We refer to Appendix B for the proof of Theorem 3.

#### IV. APPLICATION: CERTIFICATION OF BB84-SOURCES

Theorem 3 can be used to test the effective overlap in a device-independent way, i.e., where the test equipment does not need to be trusted. Such a test could, for example, be used by manufacturers to certify the quality of a source creating BB84-states [3] and to proof to a skeptical audience that their devices fulfill the desired specifications. Sources of BB84-states are widely used in quantum cryptography, including quantum key distribution and bit commitment or oblivious transfer secure in the bounded/noisy storage model [12, 27]. Moreover, recent security proofs for quantum key distribution [5, 51, 52] are based on uncertainty relations of the form (2). The overlap of the source enters there as the crucial parameter determining the secrecy of the resulting key — in particular, there is no need to do tomography of the produced states. For this reason, the overlap can be regarded as the key parameter quantifying the quality of sources of BB84-states.

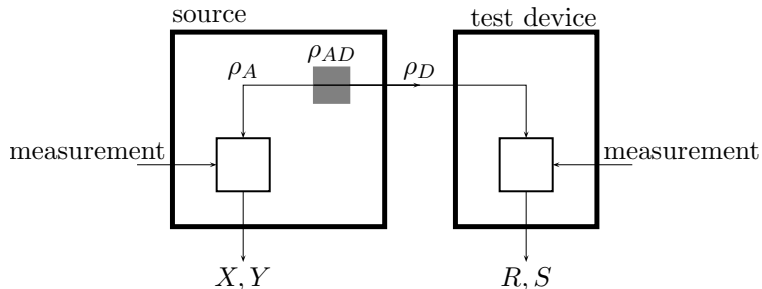


FIG. 2. Certification of entanglement-based sources of BB84-states.

Consider a (potentially imperfect) source that creates BB84-states in the following way (see Figure 2). First, it produces two entangled particles in a state  $\rho_{AD}$ , e.g. through parametric down-conversion [24, 47]. Then, it emits one part,  $D$ , of the entangled quantum state and measures the other part,  $A$ , using one of two different measurements chosen at random. Denote the binary measurement outcome by  $X$  or  $Y$  depending on the input. The input of the source thus corresponds to the choice of basis for the BB84-states, and, together with the output, defines which of the 4 states was actually prepared. Sources of this type are the subject of recent research, e.g. they



are used as heralded single photon sources [41, 59] and have applications in (device-independent) quantum cryptography [11, 19, 40].

A source which repeatedly and independently prepares states in this way can be certified by a test device which measures the emitted particle  $D$  in one of two bases chosen at random and outputs the measurement result, denoted by  $R$  or  $S$  depending on the input. The effective overlap of the source can then be estimated from the fraction  $p = k/N$  of times the CHSH condition is satisfied (i.e., either  $X = R$ ,  $X = S$ ,  $Y = R$  or  $Y \neq S$ ), as

$$c^* \approx \frac{1}{2} + 2(2p - 1) \sqrt{\frac{1}{2} - (2p - 1)^2}.$$

The precise evaluation of the statistics is straightforward but beyond the scope of this work.

## V. CONCLUSION

We have found a novel relation between the local uncertainty of measurement outcomes (expressed in terms of the von Neumann or smooth min- and max-entropy) and nonlocality (expressed in terms of the CHSH value). This relation provides analytical bounds on the unpredictability of local measurement outcomes and opens a new avenue for device-independent quantum cryptography. Namely, it enhances the cryptographic applications of the entropic uncertainty relations since the crucial parameter, the effective overlap, can be tested experimentally.

Our result is limited to the CHSH Bell test and thus only considers binary measurements. Hence, a note of caution is advised here. The CHSH value is naturally determined using measurements with binary outcomes. In practical experimental situations, however, often a third result occurs indicating that the measurement was unsuccessful. There are different ways to deal with this situation. If we randomly or deterministically assign one of the binary outcomes to this event, we stay in the framework of binary POVMs and the calculated  $\beta$  indeed gives an upper bound on the effective overlap. If these unwanted results are simply discarded, however, we open the so-called post-selection loophole and our result does not apply without further analysis.

It remains an open question whether other Bell tests can be employed to bound the effective overlap of measurements with more than two outcomes.

## ACKNOWLEDGEMENTS

We thank Michał Horodecki, Charles Ci Wen Lim, Corsin Pfister, Renato Renner, Lídia del Rio, Stephanie Wehner, Severin Winkler for helpful comments and discussions. EH and MT acknowledge support from the National Research Foundation (Singapore), and the Ministry of Education (Singapore). MT is also supported by the Swiss National Science Foundation through the National Centre of Competence in Research ‘Quantum Science and Technology’.

- 
- [1] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani. Device-Independent Security of Quantum Cryptography against Collective Attacks. *Phys. Rev. Lett.*, 98(23), 2007. DOI: [10.1103/PhysRevLett.98.230501](https://doi.org/10.1103/PhysRevLett.98.230501).
  - [2] J. S. Bell. On the Einstein-Podolsky-Rosen paradox. *Physics*, 1:195–200, 1964.
  - [3] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proc. IEEE Int. Conf. on Comp., Sys. and Signal Process.*, pages 175–179, Bangalore, 1984. IEEE.

- [4] C. H. Bennett, G. Brassard, and N. D. Mermin. Quantum cryptography without Bells theorem. *Phys. Rev. Lett.*, 68(5):557–559, Feb. 1992. DOI: [10.1103/PhysRevLett.68.557](https://doi.org/10.1103/PhysRevLett.68.557).
- [5] M. Berta, M. Christandl, R. Colbeck, J. M. Renes, and R. Renner. The Uncertainty Principle in the Presence of Quantum Memory. *Nat. Phys.*, 6(9):659–662, July 2010. DOI: [10.1038/nphys1734](https://doi.org/10.1038/nphys1734).
- [6] S. Boyd and L. Vandenberghe. *Convex Optimization*. Cambridge University Press, 2004.
- [7] J. Clauser, M. Horne, A. Shimony, and R. Holt. Proposed Experiment to Test Local Hidden-Variable Theories. *Phys. Rev. Lett.*, 23(15):880–884, Oct. 1969. DOI: [10.1103/PhysRevLett.23.880](https://doi.org/10.1103/PhysRevLett.23.880).
- [8] R. Colbeck and A. Kent. Private Randomness Expansion with Untrusted Devices. *J. Phys. A: Math. Gen.*, 44(9):095305, Mar. 2011. DOI: [10.1088/1751-8113/44/9/095305](https://doi.org/10.1088/1751-8113/44/9/095305).
- [9] P. Coles, L. Yu, V. Gheorghiu, and R. Griffiths. Information-theoretic treatment of tripartite systems and quantum channels. *Phys. Rev. A*, 83(6), June 2011. DOI: [10.1103/PhysRevA.83.062338](https://doi.org/10.1103/PhysRevA.83.062338).
- [10] P. J. Coles, R. Colbeck, L. Yu, and M. Zwoiak. Uncertainty Relations from Simple Entropic Properties. Dec. 2011. [arXiv: 1112.0543](https://arxiv.org/abs/1112.0543).
- [11] M. Curty and T. Moroder. Heralded-qubit amplifiers for practical device-independent quantum key distribution. *Phys. Rev. A*, 84(1), July 2011. DOI: [10.1103/PhysRevA.84.010304](https://doi.org/10.1103/PhysRevA.84.010304).
- [12] I. B. Damgård, S. Fehr, L. Salvail, and C. Schaffner. Cryptography in the Bounded-Quantum-Storage Model. *SIAM J. Comput.*, 37(6):1865, 2008. DOI: [10.1137/060651343](https://doi.org/10.1137/060651343).
- [13] I. B. Damgaard, S. Fehr, R. Renner, L. Salvail, and C. Schaffner. A Tight High-Order Entropic Quantum Uncertainty Relation With Applications. In *Proc. CRYPTO*, volume 4622 of *LNCS*, pages 360–378. Springer, Dec. 2007.
- [14] N. Datta. Min- and Max- Relative Entropies and a New Entanglement Monotone. *IEEE Trans. on Inf. Theory*, 55(6):2816–2826, 2009. DOI: [10.1109/TIT.2009.2018325](https://doi.org/10.1109/TIT.2009.2018325).
- [15] D. Deutsch. Uncertainty in Quantum Measurements. *Phys. Rev. Lett.*, 50(9):631–633, Feb. 1983. DOI: [10.1103/PhysRevLett.50.631](https://doi.org/10.1103/PhysRevLett.50.631).
- [16] I. Devetak and A. Winter. Classical Data Compression with Quantum Side Information. *Phys. Rev. A*, 68(4), Oct. 2003. DOI: [10.1103/PhysRevA.68.042301](https://doi.org/10.1103/PhysRevA.68.042301).
- [17] F. Dupuis, M. Berta, J. Wullschleger, and R. Renner. The Decoupling Theorem. Dec. 2010. [arXiv: 1012.6044](https://arxiv.org/abs/1012.6044).
- [18] A. Einstein, B. Podolsky, and N. Rosen. Can Quantum-Mechanical Description of Physical Reality Be Considered Complete? *Phys. Rev.*, 47:777–780, May 1935.
- [19] N. Gisin, S. Pironio, and N. Sangouard. Proposal for Implementing Device-Independent Quantum Key Distribution Based on a Heralded Qubit Amplifier. *Phys. Rev. Lett.*, 105(7), Aug. 2010. DOI: [10.1103/PhysRevLett.105.070501](https://doi.org/10.1103/PhysRevLett.105.070501).
- [20] E. Hänggi and R. Renner. Device-Independent Quantum Key Distribution with Commuting Measurements. Sept. 2010. [arXiv: 1009.1833](https://arxiv.org/abs/1009.1833).
- [21] W. Heisenberg. Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik. *Z. Phys.*, 43(3-4):172–198, Mar. 1927.
- [22] M. Horodecki. Personal Communication, 2011.
- [23] C. Jordan. Essai sur la géométrie à n dimensions. *Bulletin de la S.M.F.*, 3:103–174, 1875.
- [24] T. E. Kiess, Y. H. Shih, A. V. Sergienko, and C. O. Alley. Einstein-Podolsky-Rosen-Bohm experiment using pairs of light quanta produced by type-II parametric down-conversion. *Phys. Rev. Lett.*, 71(24):3893–3897, Dec. 1993. DOI: [10.1103/PhysRevLett.71.3893](https://doi.org/10.1103/PhysRevLett.71.3893).
- [25] M. Koashi. Unconditional Security of Quantum Key Distribution and the Uncertainty Principle. *J. Phys. Conf. Ser.*, 36(1):98–102, Apr. 2006.
- [26] R. König, R. Renner, and C. Schaffner. The Operational Meaning of Min- and Max-Entropy. *IEEE Trans. on Inf. Theory*, 55(9):4337–4347, Sept. 2009. DOI: [10.1109/TIT.2009.2025545](https://doi.org/10.1109/TIT.2009.2025545).
- [27] R. König, S. Wehner, and J. Wullschleger. Unconditional Security From Noisy Quantum Storage. *IEEE Trans. on Inf. Theory*, 58(3):1962–1984, Mar. 2012. DOI: [10.1109/TIT.2011.2177772](https://doi.org/10.1109/TIT.2011.2177772).
- [28] M. Krishna and K. R. Parthasarathy. An Entropic Uncertainty Principle for Quantum Measurements. *Indian J. Stat.*, 64(3):842–851, Oct. 2002.
- [29] E. H. Lieb and M. B. Ruskai. Proof of the strong subadditivity of quantum-mechanical entropy. *J. Math. Phys.*, 14(12):1938, Dec. 1973. DOI: [10.1063/1.1666274](https://doi.org/10.1063/1.1666274).
- [30] C. C. W. Lim and Others. Manuscript in Preparation, 2012.
- [31] H. Maassen and J. Uffink. Generalized entropic uncertainty relations. *Phys. Rev. Lett.*, 60(12):1103–1106, Mar. 1988. DOI: [10.1103/PhysRevLett.60.1103](https://doi.org/10.1103/PhysRevLett.60.1103).

- [32] F. Magniez, D. Mayers, and M. Mosca. Self-Testing of Quantum Circuits. In *Proc. ICALP*, pages 72–83, 2006.
- [33] L. Masanes. Asymptotic Violation of Bell Inequalities and Distillability. *Phys. Rev. Lett.*, 97(5), Aug. 2006. DOI: [10.1103/PhysRevLett.97.050503](https://doi.org/10.1103/PhysRevLett.97.050503).
- [34] L. Masanes, S. Pironio, and A. Acín. Secure device-independent quantum key distribution with causally independent measurement devices. *Nat. Commun.*, 2:238, Mar. 2011. DOI: [10.1038/ncomms1244](https://doi.org/10.1038/ncomms1244).
- [35] D. Mayers and A. Yao. Quantum Cryptography with Imperfect Apparatus. In *Proc. FOCS*, pages 503–509, 1998.
- [36] D. Mayers and A. Yao. Self Testing Quantum Apparatus. *Quant. Inf. Comput.*, 4(4):273—286, 2004.
- [37] M. McKague and M. Mosca. Generalized Self-Testing and the Security of the 6-State Protocol. In *Proc. TQC*, pages 113–130, June 2010. arXiv: [1006.0150](https://arxiv.org/abs/1006.0150).
- [38] A. Neumark. On a Representation of Additive Operator Set Functions. *Acad. Sci. URSS*, 41:359–361, 1943.
- [39] J. Oppenheim and S. Wehner. The Uncertainty Principle Determines the Nonlocality of Quantum Mechanics. *Science*, 330(6007):1072–1074, Nov. 2010. DOI: [10.1126/science.1192065](https://doi.org/10.1126/science.1192065).
- [40] D. Pitkanen, X. Ma, R. Wickert, P. van Loock, and N. Lütkenhaus. Efficient heralding of photonic qubits with applications to device-independent quantum key distribution. *Phys. Rev. A*, 84(2), Aug. 2011. DOI: [10.1103/PhysRevA.84.022325](https://doi.org/10.1103/PhysRevA.84.022325).
- [41] T. Pittman, B. Jacobs, and J. Franson. Heralding single photons from pulsed parametric down-conversion. *Optics Commun.*, 246(4-6):545–550, Feb. 2005. DOI: [10.1016/j.optcom.2004.11.027](https://doi.org/10.1016/j.optcom.2004.11.027).
- [42] J. M. Renes and R. Renner. One-Shot Classical Data Compression With Quantum Side Information and the Distillation of Common Randomness or Secret Keys. *IEEE Trans. on Inf. Theory*, 58(3):1985–1991, Mar. 2012. DOI: [10.1109/TIT.2011.2177589](https://doi.org/10.1109/TIT.2011.2177589).
- [43] R. Renner. *Security of Quantum Key Distribution*. PhD thesis, ETH Zurich, Dec. 2005. arXiv: [quant-ph/0512258](https://arxiv.org/abs/quant-ph/0512258).
- [44] H. P. Robertson. The Uncertainty Principle. *Phys. Rev.*, 34(1):163–164, July 1929. DOI: [10.1103/PhysRev.34.163](https://doi.org/10.1103/PhysRev.34.163).
- [45] M. Seevinck and J. Uffink. Local commutativity versus Bell inequality violation for entangled states and versus non-violation for separable states. *Phys. Rev. A*, 76(4):1–6, Oct. 2007. DOI: [10.1103/PhysRevA.76.042105](https://doi.org/10.1103/PhysRevA.76.042105).
- [46] C. Shannon. A Mathematical Theory of Communication. *Bell Syst. Tech. J.*, 27:379–423, 1948.
- [47] Y. H. Shih and C. O. Alley. New Type of Einstein-Podolsky-Rosen-Bohm Experiment Using Pairs of Light Quanta Produced by Optical Parametric Down Conversion. *Phys. Rev. Lett.*, 61(26):2921–2924, Dec. 1988. DOI: [10.1103/PhysRevLett.61.2921](https://doi.org/10.1103/PhysRevLett.61.2921).
- [48] M. Tomamichel. *A Framework for Non-Asymptotic Quantum Information Theory*. Phd thesis, ETH Zurich, 2012.
- [49] M. Tomamichel, R. Colbeck, and R. Renner. A Fully Quantum Asymptotic Equipartition Property. *IEEE Trans. on Inf. Theory*, 55(12):5840–5847, Dec. 2009. DOI: [10.1109/TIT.2009.2032797](https://doi.org/10.1109/TIT.2009.2032797).
- [50] M. Tomamichel, R. Colbeck, and R. Renner. Duality Between Smooth Min- and Max-Entropies. *IEEE Trans. on Inf. Theory*, 56(9):4674–4681, Sept. 2010. DOI: [10.1109/TIT.2010.2054130](https://doi.org/10.1109/TIT.2010.2054130).
- [51] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner. Tight Finite-Key Analysis for Quantum Cryptography. *Nat. Commun.*, 3:634, Jan. 2012. DOI: [10.1038/ncomms1631](https://doi.org/10.1038/ncomms1631).
- [52] M. Tomamichel and R. Renner. Uncertainty Relation for Smooth Entropies. *Phys. Rev. Lett.*, 106(11), Mar. 2011. DOI: [10.1103/PhysRevLett.106.110506](https://doi.org/10.1103/PhysRevLett.106.110506).
- [53] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner. Leftover Hashing Against Quantum Side Information. *IEEE Trans. on Inf. Theory*, 57(8):5524–5535, Aug. 2011. DOI: [10.1109/TIT.2011.2158473](https://doi.org/10.1109/TIT.2011.2158473).
- [54] B. S. Tsirelson. Quantum generalizations of Bell’s inequality. *Lett. Math. Phys.*, 4(2):93–100, 1980.
- [55] B. S. Tsirelson. Some Results and Problems on Quantum Bell-Type Inequalities. *Hadronic J. Supp.*, 8(4):329–345, 1993.
- [56] S. Wehner. Tsirelson Bounds for Generalized Clauser-Horne-Shimony-Holt Inequalities. *Phys. Rev. A*, 73(2), Feb. 2006. DOI: [10.1103/PhysRevA.73.022110](https://doi.org/10.1103/PhysRevA.73.022110).
- [57] S. Wehner. *Cryptography in a Quantum World*. PhD thesis, Universiteit van Amsterdam, Feb. 2008. arXiv: [0806.3483](https://arxiv.org/abs/0806.3483).
- [58] S. Wehner and A. Winter. Entropic Uncertainty Relations—A Survey. *New J. Phys.*, 12(2):025009, Feb. 2010. DOI: [10.1088/1367-2630/12/2/025009](https://doi.org/10.1088/1367-2630/12/2/025009).

- [59] G. Y. Xiang, T. C. Ralph, A. P. Lund, N. Walk, and G. J. Pryde. Heralded noiseless linear amplification and distillation of entanglement. *Nat. Photon.*, 4(5):316–319, Mar. 2010. DOI: [10.1038/nphoton.2010.35](https://doi.org/10.1038/nphoton.2010.35).

## Appendix A: Proof of Generalized Uncertainty Relations

### 1. Preliminaries

For the proof, we need two conditional entropies that are generalizations of the von Neumann entropy, the smooth min- and max-entropy. In order to define these, we first need to introduce the concept of sub-normalized quantum states and the purified distance. A sub-normalized quantum state is a positive semidefinite operator  $\rho$  with  $0 < \text{tr}(\rho) \leq 1$  on a Hilbert space.

The *purified distance* [50] between two sub-normalized quantum states,  $\rho$  and  $\tau$ , is given by  $P(\rho, \tau) := \sqrt{1 - F^2(\rho, \tau)}$ , where  $F(\rho, \tau) := \text{tr} |\sqrt{\rho}\sqrt{\tau}| + \sqrt{(1 - \text{tr} \rho)(1 - \text{tr} \tau)}$  is the generalized fidelity. We say that the two states are  $\varepsilon$ -close, denoted  $\rho \approx^\varepsilon \tau$ , if and only if  $P(\rho, \tau) \leq \varepsilon$ . The purified distance is a metric and has various important properties, e.g.  $\rho \approx^\varepsilon \tau \implies \mathcal{E}(\rho) \approx^\varepsilon \mathcal{E}(\tau)$  for all trace non-increasing completely positive maps  $\mathcal{E}$  [50].

Furthermore, due to Uhlmann's theorem, there exists an extension  $\tau_{AB}$  of  $\tau_A = \text{tr}_B(\tau_{AB})$  such that  $P(\rho_{AB}, \tau_{AB}) = P(\rho_A, \tau_A)$  for any bipartite state  $\rho_{AB}$ . This state can be constructed (see [17], Lemma B.2) and has the form

$$\tau_{AB} = (X_A \otimes \mathbb{1}_B) \rho_{AB} (X_A^\dagger \otimes \mathbb{1}_B) \quad (\text{A1})$$

for some linear operator  $X_A$  on  $A$ . We use ' $\succeq$ ' to denote the positive semidefinite partial order on Hermitian matrices, i.e.  $A \succeq B$  if and only if  $A - B$  is positive semidefinite.

*Definition 3.* Let  $\rho_{AB}$  be a sub-normalized state. The *min-entropy* of  $A$  given  $B$  is [43]

$$H_{\min}(A|B)_\rho := \max_{\sigma_B} \sup \{ \lambda \in \mathbb{R} : \rho_{AB} \preceq 2^{-\lambda} \mathbb{1}_A \otimes \sigma_B \},$$

where the maximization is over all states  $\sigma_B$  on  $B$ . For  $\varepsilon \geq 0$ , the  $\varepsilon$ -smooth min-entropy and the  $\varepsilon$ -smooth max-entropy of  $A$  given  $B$  are defined as [26, 50]

$$H_{\min}^\varepsilon(A|B)_\rho := \max_{\tilde{\rho}} H_{\min}(A|B)_{\tilde{\rho}} \quad \text{and} \quad H_{\max}^\varepsilon(A|B)_\rho := -H_{\min}^\varepsilon(A|C)_\rho$$

where the optimization is over all sub-normalized states  $\tilde{\rho}_{AB} \approx^\varepsilon \rho_{AB}$  and  $\rho_{ABC}$  is an arbitrary purification of  $\rho_{AB}$ .

We note that in the limit of many independent copies of a quantum state,  $\tau_{A^n B^n} = \rho_{AB}^{\otimes n}$ , the smooth entropies converge to the von Neumann entropy [48, 49]. For any  $0 < \varepsilon < 1$ ,

$$\lim_{n \rightarrow \infty} \frac{1}{n} H_{\min}^\varepsilon(A^n|B^n)_\tau = \lim_{n \rightarrow \infty} \frac{1}{n} H_{\max}^\varepsilon(A^n|B^n)_\tau = H(A|B)_\rho. \quad (\text{A2})$$

The smooth entropies satisfy various data-processing inequalities, in particular, for every CPTPM  $\mathcal{E}$  from  $B$  to  $B'$ , we have [50]

$$H_{\min}^\varepsilon(A|B)_\rho \leq H_{\min}^\varepsilon(A|B')_\tau \quad \text{and} \quad H_{\max}^\varepsilon(A|B)_\rho \leq H_{\max}^\varepsilon(A|B')_\tau \quad \text{for } \tau_{AB'} = \mathcal{E}[\rho_{AB}]. \quad (\text{A3})$$

Finally, we need the following result. (See also [48] for a slightly more general statement.)

**Lemma 4.** Let  $M_{AB} \succeq 0$  and let  $\{E_A^k\}_k$  be a set of linear operators on  $A$ . Then,

$$\text{tr}_A \left( \sum_k (E_A^k \otimes \mathbb{1}_B) M_{AB} (E_A^{k\dagger} \otimes \mathbb{1}_B) \right) \preceq \left\| \sum_k E_A^{k\dagger} E_A^k \right\| \text{tr}_A(M_{AB}). \quad (\text{A4})$$

*Proof.* Due to the linearity and cyclicity of the partial trace, we have

$$\mathrm{tr}_A \left( \sum_k (E_A^k \otimes \mathbb{1}_B) M_{AB} (E_A^{k\dagger} \otimes \mathbb{1}_B) \right) = \mathrm{tr}_A \left( \sum_k (E_A^{k\dagger} E_A^k \otimes \mathbb{1}_B) M_{AB} \right)$$

We introduce the operator  $R_A = \mathbb{1}_A \left\| \sum_k E_A^{k\dagger} E_A^k \right\| - \sum_k E_A^{k\dagger} E_A^k \succeq 0$ . We note that  $\mathrm{tr}_A ((\sqrt{R_A} \otimes \mathbb{1}_B) M_{AB} (\sqrt{R_A} \otimes \mathbb{1}_B)) \succeq 0$  and, thus,

$$\begin{aligned} \mathrm{tr}_A \left( \sum_k (E_B^k \dagger E_B^k \otimes \mathbb{1}_B) M_{AB} \right) &\preceq \mathrm{tr}_A \left( \sum_k ((E_B^k \dagger E_B^k + R_A) \otimes \mathbb{1}_B) M_{AB} \right) \\ &= \left\| \sum_k E_A^{k\dagger} E_A^k \right\| \mathrm{tr}_A(M_{AB}). \end{aligned} \quad \square$$

## 2. Smooth Relative Entropy

Our proof relies heavily on the following auxiliary quantity, related to the relative max-entropy [14],  $h_{\min}(\rho \|\sigma) := \sup\{\lambda \in \mathbb{R} : \rho \preceq 2^{-\lambda} \sigma\}$ . It is easy to see that this quantity is monotonic under the application of a quantum map, i.e.  $h_{\min}(\mathcal{E}[\rho] \|\mathcal{E}[\sigma]) \geq h_{\min}(\rho \|\sigma)$  for all CPTPMs  $\mathcal{E}$ .

The following lemma relates the min-entropy and the relative entropy of the state and its marginal. (We refer to [53] for a proof.)

**Lemma 5.** *Let  $\varepsilon > 0$  and  $\rho_{ABC}$  a pure quantum state. Then, there exists a projector  $\Pi_{AC}$  and a state  $\tilde{\rho}_{ABC} = (\Pi_{AC} \otimes \mathbb{1}_B) \rho_{ABC} (\Pi_{AC} \otimes \mathbb{1}_B)$  such that  $\tilde{\rho}_{ABC} \approx^\varepsilon \rho_{ABC}$  and*

$$h_{\min}(\tilde{\rho}_{AB} \|\mathbb{1}_A \otimes \rho_B) \geq H_{\min}(A|B)_\rho - \log_2(2/\varepsilon^2).$$

The next lemma provides a similar upper bound for the smooth min-entropy.

**Lemma 6.** *Let  $\varepsilon > 0, \varepsilon' \geq 0$  and  $\rho_{AB}$  a quantum state. Then, there exists a state  $\bar{\rho}_{AB}$  with  $P(\bar{\rho}_{AB}, \rho_{AB}) \leq \varepsilon + 2\varepsilon'$  such that*

$$h_{\min}(\bar{\rho}_{AB} \|\mathbb{1}_A \otimes \rho_B) \geq H_{\min}^{\varepsilon'}(A|B)_\rho - \log_2(2/\varepsilon^2).$$

*Proof.* Let  $\rho_{ABC}$  and  $\hat{\rho}_{ABC} \approx^{\varepsilon'} \rho_{ABC}$  be pure states such that  $H_{\min}^{\varepsilon'}(A|B)_\rho = H_{\min}(A|B)_{\hat{\rho}}$ . We apply Lemma 5 to this state to get  $h_{\min}(\tilde{\rho}_{AB} \|\mathbb{1}_A \otimes \hat{\rho}_B) \geq h_{\min}^{\varepsilon'}(A|B)_\rho - \log_2(2/\varepsilon^2)$ , where  $|\tilde{\rho}_{ABC}\rangle = (\Pi_{AC} \otimes \mathbb{1}_B) |\hat{\rho}_{ABC}\rangle$  and  $\tilde{\rho}_{ABC} \approx^\varepsilon \hat{\rho}_{ABC}$ . Using Eq. (A1), we define the operator  $X_B$  with the property  $X_B \hat{\rho}_B X_B^\dagger = \rho_B$ ; hence  $X_B \hat{\rho}_{ABC} X_B^\dagger \approx^{\varepsilon'} \hat{\rho}_{ABC}$ .

Applying this to the defining operator inequality of the relative entropy above leads to

$$\tilde{\rho}_{AB} \preceq 2^{-\lambda} \mathbb{1}_A \otimes \hat{\rho}_B \implies \underbrace{X_B \tilde{\rho}_{AB} X_B^\dagger}_{=:\bar{\rho}_{AB}} \preceq 2^{-\lambda} \mathbb{1}_A \otimes \rho_B$$

and, thus,  $h_{\min}(\tilde{\rho}_{AB} \|\mathbb{1}_A \otimes \hat{\rho}_B) \leq h_{\min}(\bar{\rho}_{AB} \|\mathbb{1}_A \otimes \rho_B)$ . Furthermore,  $\bar{\rho}_{AB}$  is sub-normalized since  $\mathrm{tr}(\bar{\rho}_B) = \mathrm{tr}(X_B \tilde{\rho}_B X_B^\dagger) \leq \mathrm{tr}(X_B \hat{\rho}_B X_B^\dagger) = \mathrm{tr}(\rho_B) \leq 1$ . Hence, it remains to bound  $P(\bar{\rho}_{AB}, \rho_{AB}) \leq P(\bar{\rho}_{AB}, \tilde{\rho}_{AB}) + P(\tilde{\rho}_{AB}, \hat{\rho}_{AB}) + P(\hat{\rho}_{AB}, \rho_{AB}) \leq P(\bar{\rho}_{AB}, \tilde{\rho}_{AB}) + \varepsilon + \varepsilon'$ . We have

$$\begin{aligned} P(\bar{\rho}_{AB}, \tilde{\rho}_{AB}) &= P((X_B \otimes \Pi_{AC}) \hat{\rho}_{ABC} (X_B^\dagger \otimes \Pi_{AC}), (\Pi_{AC} \otimes \mathbb{1}_B) \hat{\rho}_{ABC} (\Pi_{AC} \otimes \mathbb{1}_B)) \\ &\leq P(X_B \hat{\rho}_B X_B^\dagger, \hat{\rho}_B) \leq \varepsilon', \end{aligned}$$

where we used the monotonicity of the purified distance under projections.  $\square$



### 3. Uncertainty of Two Consecutive Measurements

We prove a more general result that implies Theorem 2. For this purpose, we consider two consecutive measurements applied to the  $A$  system and a state  $\rho_{ABC}$ : a projective measurement,  $\mathsf{K} = \{P_A^k\}_k$ , followed by either one of two POVMs,  $\mathsf{X} = \{M_A^x\}_x$  or  $\mathsf{Y} = \{N_A^y\}_y$ . More precisely, we are interested in the post measurement states

$$\rho_{XKB} = \sum_{x,k} |x\rangle\langle x| \otimes |k\rangle\langle k| \otimes \text{tr}_{AC} \left( (P_A^k M_A^x P_A^k \otimes \mathbb{1}_{BC}) \rho_{ABC} \right) \quad \text{and} \quad (\text{A5})$$

$$\rho_{YKC} = \sum_{y,k} |y\rangle\langle y| \otimes |k\rangle\langle k| \otimes \text{tr}_{AB} \left( (P_A^k N_A^y P_A^k \otimes \mathbb{1}_{BC}) \rho_{ABC} \right). \quad (\text{A6})$$

**Proposition 7.** *Let  $\rho_{ABC}$  be a tripartite quantum state, let  $\varepsilon \geq 0$  and let  $\bar{\varepsilon} > 0$ . Moreover, let  $\mathsf{K} = \{P_A^k\}_k$  be a projective measurement and  $\mathsf{X} = \{M_A^x\}_x$  and  $\mathsf{Y} = \{N_A^y\}_y$  be two POVMs on  $A$ . Then, the post measurement states (A5) and (A6) satisfy*

$$H_{\min}^{\varepsilon+2\bar{\varepsilon}}(X|BK)_\rho + H_{\max}^\varepsilon(Y|CK)_\rho \geq -\log_2 c_{\mathsf{K}}^*(\rho_A, \mathsf{X}, \mathsf{Y}) - \log_2(2/\bar{\varepsilon}^2), \quad (\text{A7})$$

where  $c_{\mathsf{K}}^*(\rho_A, \mathsf{X}, \mathsf{Y}) := \sum_k \text{tr}(P_A^k \rho_A) \max_x \left\| \sum_y P_A^k N_A^y P_A^k \cdot P_A^k M_A^x P_A^k \cdot P_A^k N_A^y P_A^k \right\|$ .

*Proof.* We first prove the statement for pure  $\rho_{ABC}$ . Then, for mixed states, we consider a purification  $\rho_{ABCE}$  of  $\rho_{ABC}$ , for which the theorem holds and take the partial trace over  $E$ . As this cannot decrease the smooth entropies (A3), the generalization follows.

We consider the Stinespring dilation of the joint measurement of  $\mathsf{X}$  and  $\mathsf{K}$ , denoted  $U$ , which coherently stores the measurement outcome of  $\mathsf{X}$  in registers  $X$  and  $X'$  and the measurement outcome of  $\mathsf{K}$  in  $K$  and  $K'$ , i.e.  $U := \sum_{x,k} |x\rangle_X \otimes |x\rangle_{X'} \otimes |k\rangle_K \otimes |k\rangle_{K'} \otimes \sqrt{M_A^x} P_A^k$ . Similarly, we introduce the Stinespring dilation of the joint measurement of  $\mathsf{Y}$  and  $\mathsf{K}$ , and the partial isometry  $W := UV^\dagger$  which, using  $P_A^k P_A^{k'} = \delta_{kk'} P_A^k$ , evaluates to

$$W = \sum_{x,y,k} |x\rangle\langle y| \otimes |x\rangle\langle y| \otimes |k\rangle\langle k| \otimes |k\rangle\langle k| \otimes \sqrt{M_A^x} P_A^k \sqrt{N_A^y}. \quad (\text{A8})$$

These isometries allow us to introduce the states  $\rho_{AXX'KK'BC} = U\rho_{ABC}U^\dagger$  and, analogously,  $\rho_{AYY'KK'BC} = V\rho_{ABC}V^\dagger$ , whose marginals correspond to the post measurement states  $\rho_{XKB}$  and  $\rho_{YKC}$  of (A5) and (A6), respectively.

The proof now proceeds in several steps. First, we reformulate the statement of the theorem in terms of smooth min-entropies using the definition of the smooth max-entropy. Then, we use Lemma 6 to find an upper bound on one of the entropies in terms of a relative entropy of the state and its marginal. The structure of the marginal can then be used to extract  $c_{\mathsf{K}}^*$ .

Due to the duality [50] between smooth min- and max-entropy, the statement of the proposition is equivalent to  $H_{\min}^{2\varepsilon+\bar{\varepsilon}}(X|KB)_\rho \geq H_{\min}^\varepsilon(Y|AY'K'B)_\rho - \log_2 c_{\mathsf{K}}^* - \log_2(2/\bar{\varepsilon}^2)$ . Applying Lemma 6, we introduce a state  $\tilde{\rho} \approx^{2\varepsilon+\bar{\varepsilon}} \rho$  such that

$$h_{\min}(\tilde{\rho}_{AYY'K'B} \| \mathbb{1}_Y \otimes \rho_{AY'K'B}) \geq H_{\min}^\varepsilon(Y|AY'K'B)_\rho - \log_2(2/\bar{\varepsilon}^2).$$

Next, we use the monotonicity of  $h_{\min}$  under trace-preserving completely positive maps to measure the  $K'$  system. More precisely, we apply the map  $\mathcal{M} : \rho \mapsto \sum_k |k\rangle\langle k|_{K'} \rho |k\rangle\langle k|_{K'}$  to both arguments in  $h_{\min}$  above. This has no effect on  $\rho_{AY'K'B}$ , which is classical on  $K'$  by definition. Using the state  $\bar{\rho}_{AYY'K'B} = \mathcal{M}[\tilde{\rho}_{AYY'K'B}]$ , we thus have

$$\underbrace{h_{\min}(\bar{\rho}_{AYY'K'B} \| \mathbb{1}_Y \otimes \rho_{AY'K'B})}_{=: \lambda} \geq H_{\min}^\varepsilon(Y|AY'K'B)_\rho - \log_2(2/\bar{\varepsilon}^2). \quad (\text{A9})$$

Moreover, the purified distance satisfies  $P(\bar{\rho}, \rho) \leq P(\tilde{\rho}, \rho) \leq 2\varepsilon + \bar{\varepsilon}$ .

From the definition of  $h_{\min}$ , we get

$$\bar{\rho}_{AY'K'B} \preceq 2^{-\lambda} \mathbb{1}_Y \otimes \rho_{AY'K'B}, \quad (\text{A10})$$

where we employed the marginal state  $\rho_{AY'K'B} = \text{tr}_{YK'}(V\rho_{AB}V^\dagger) = \sum_{y,k} \sqrt{N_A^y} P_A^k \rho_{AB} P_A^k \sqrt{N_A^y} \otimes |k\rangle\langle k| \otimes |y\rangle\langle y|$ . Taking the tensor product with  $\mathbb{1}_K$  on both sides of (A10), conjugating the resulting inequality with  $W$  and taking the partial trace over  $A, Y'$  and  $K'$  leads to

$$\underbrace{\text{tr}_{AX'K'}(W(\bar{\rho}_{AY'Y'K'B} \otimes \mathbb{1}_K)W^\dagger)}_{=: \bar{\tau}_{XKB}} \preceq 2^{-\lambda} \text{tr}_{AX'K}(W(\mathbb{1}_{YK} \otimes \rho_{AY'K'B})W^\dagger). \quad (\text{A11})$$

We evaluate the trace term on the rhs. of (A11) to get

$$\begin{aligned} & \text{tr}_{AX'K'}(W(\mathbb{1}_{YK} \otimes \rho_{AY'K'B})W^\dagger) \\ &= \sum_{x,y,k} |x\rangle\langle x| \otimes |k\rangle\langle k| \otimes \langle yk| \text{tr}_A(\sqrt{M_A^x} P_A^k \sqrt{N_A^y} \rho_{AY'K'B} \sqrt{N_A^y} P_A^k \sqrt{M_A^x}) |yk\rangle \\ &= \sum_x |x\rangle\langle x| \otimes \sum_k |k\rangle\langle k| \otimes \text{tr}_A\left(\sum_y \sqrt{M_A^x} P_A^k N_A^y P_A^k \rho_{AB} P_A^k N_A^y P_A^k \sqrt{M_A^x}\right) \\ &\leq \mathbb{1}_X \otimes \underbrace{\sum_k |k\rangle\langle k| \otimes \max_x \left\| \sum_y P_A^k N_A^y P_A^k M_A^x P_A^k N_A^y P_A^k \right\| \text{tr}_A(P_A^k \rho_{AB})}_{=: \tilde{\omega}_{KB}} \end{aligned} \quad (\text{A12})$$

We used Lemma 4 to arrive at (A12). Note that  $\text{tr}(\tilde{\omega}_{KB}) = c_K^*$ ; hence, we choose  $\omega_{KB} = \tilde{\omega}_{KB}/c_K^*$  and employ (A11) to find a lower bound on  $h_{\min}(\bar{\tau}_{XKB} \|\mathbb{1}_X \otimes \omega_{KB})$  in terms of  $\lambda$  and  $c_K^*$ , i.e.

$$\begin{aligned} h_{\min}(\bar{\tau}_{XKB} \|\mathbb{1}_X \otimes \omega_{KB}) &\geq \lambda - \log_2 c_K^* \\ &\geq H_{\min}^\varepsilon(Y|AY'K'B)_\rho - \log_2 c_K^* - \log_2(2/\bar{\varepsilon}^2). \end{aligned} \quad (\text{A13})$$

We have  $P(\bar{\tau}_{XKB}, \rho_{XKB}) = P(\bar{\rho}_{XKB}, \rho_{XKB}) \leq 2\varepsilon + \bar{\varepsilon}$ . Therefore, using the definition of the smooth min-entropy, we get  $H_{\min}^{2\varepsilon + \bar{\varepsilon}}(X|KB)_\rho \geq h_{\min}(\bar{\tau}_{XKB} \|\mathbb{1}_X \otimes \omega_{KB})$ , which, substituted into (A13), concludes the proof.  $\square$

#### 4. Proof of Theorem 2

Theorem 2 is a corollary of Proposition 7.

*Proof of Theorem 2.* Recall that the effective overlap is defined as

$$c^*(\rho_A, \mathbf{X}, \mathbf{Y}) = \inf_{U, \mathbf{X}', \mathbf{Y}', \mathbf{K}'} c_{\mathbf{K}'}^*(U\rho_A U^\dagger, \mathbf{X}', \mathbf{Y}'),$$

where the infimum is taken over all embeddings  $U$  from  $A$  to  $A'$ , all measurements  $\mathbf{X}' = \{M_{A'}^x\}_x$  and  $\mathbf{Y}' = \{N_{A'}^y\}_y$  on  $A'$  and all projective measurements  $\mathbf{K}' = \{P_{A'}^k\}_k$  such that  $\sum_k U^\dagger P_{A'}^k M_{A'}^x P_{A'}^k U = M_A^x$  and  $\sum_k U^\dagger P_{A'}^k N_{A'}^y P_{A'}^k U = N_A^y$ . Furthermore, for any such  $\{U, \mathbf{X}', \mathbf{Y}', \mathbf{K}'\}$ , Proposition 7 implies that the post measurement states

$$\tau_{XKB} = \sum_{x,k} |x\rangle\langle x| \otimes |k\rangle\langle k| \otimes \text{tr}_{A'C}((P_{A'}^k M_{A'}^x P_{A'}^k \otimes \mathbb{1}_{BC})U\rho_{ABC}U^\dagger) \quad \text{and} \quad (\text{A14})$$

$$\tau_{YKC} = \sum_{y,k} |y\rangle\langle y| \otimes |k\rangle\langle k| \otimes \text{tr}_{A'B}((P_{A'}^k N_{A'}^y P_{A'}^k \otimes \mathbb{1}_{BC})U\rho_{ABC}U^\dagger). \quad (\text{A15})$$

satisfy

$$\begin{aligned} H_{\min}^{\varepsilon+2\bar{\varepsilon}}(X|B)_\tau + H_{\max}^\varepsilon(Y|C)_\tau &\geq H_{\min}^{\varepsilon+2\bar{\varepsilon}}(X|BK)_\tau + H_{\max}^\varepsilon(Y|CK)_\tau \\ &\geq -\log_2 c_{K'}^*(U\rho_A U^\dagger, \mathbf{X}', \mathbf{Y}') - \log_2(2/\bar{\varepsilon}^2), \end{aligned}$$

where we also employed the data-processing inequality of the smooth min- and max-entropies (A3) to trace out the  $K$  system. Furthermore, the marginal states of (A14) and (A15) without  $K$  correspond to the post measurement states when measuring  $\mathbf{X}$  and  $\mathbf{Y}$  on  $\rho$ , namely

$$\begin{aligned} \text{tr}_K(\tau_{XKB}) &= \sum_x |x\rangle\langle x| \otimes \text{tr}_{AC} \left( \left( \sum_k U^\dagger P_{A'}^k M_{A'}^x P_{A'}^k U \right) \rho_{ABC} \right) \\ &= \sum_x |x\rangle\langle x| \otimes \text{tr}_{AC} (M_A^x \rho_{ABC}) = \mathcal{M}_X[\rho_{AB}] \end{aligned}$$

and, similarly,  $\text{tr}_K(\tau_{YKC}) = \mathcal{M}_Y[\rho_{AC}]$ . This implies that the uncertainty relation holds for each candidate in the minimization and, thus, also for its infimum. (The last argument implicitly uses the continuity of the function  $-\log_2(\cdot)$ .) This concludes the proof.  $\square$

## 5. Proof of Theorem 1

Theorem 1 follows as a corollary of Theorem 2 and the entropic asymptotic equipartition (A2).

*Proof of Theorem 1.* We apply Theorem 2 to the state  $\rho_{ABC}^n = \rho_{ABC}^{\otimes n}$  and use the measurements  $\mathbf{X}^n$  and  $\mathbf{Y}^n$ , which measure  $\mathbf{X}$  and  $\mathbf{Y}$  on each of the  $n$  copies, respectively. It is easy to verify that  $c^*(\rho_A^n, \mathbf{X}^n, \mathbf{Y}^n) \leq c^*(\rho_A, \mathbf{X}, \mathbf{Y})^n$  in this case. Theorem 2 applied to this situation thus yields

$$\frac{1}{n} H_{\min}^{\varepsilon+2\bar{\varepsilon}}(X^n|B^n)_\rho + \frac{1}{n} H_{\max}^\varepsilon(Y^n|C^n)_\rho \geq -\log_2 c^*(\rho_A, \mathbf{X}, \mathbf{Y}) - \frac{1}{n} \log_2(2/\bar{\varepsilon}^2).$$

Finally, taking the limit  $n \rightarrow \infty$  and employing (A2) immediately proves Theorem 1.  $\square$

## Appendix B: Proof of Relation to Nonlocality

### 1. Preliminaries

Projective measurements with binary outcomes can be described compactly as an *observable*  $O = M_0 - M_1$  with spectrum in  $\{1, -1\}$ , i.e.  $O^2 = \mathbb{1}$ . Tsirelson [54] related the correlations which can be achieved when measuring quantum systems to the existence of unit vectors in a real vector space. Namely, Tsirelson's result states that for any set of observables  $O_1, \dots, O_n$  and  $Q_1, \dots, Q_n$  with eigenvalues in the interval  $[-1, 1]$  and any bipartite pure state  $|\psi\rangle\langle\psi|$  there exist real unit vectors  $x_1, \dots, x_n, y_1, \dots, y_n \in \mathbb{R}^{2^n}$  s.t.

$$\langle\psi|O_i \otimes Q_j|\psi\rangle = x_i^\top \cdot y_j \tag{B1}$$

for all  $i, j \in [n]$ . Conversely, if there exist such real unit vectors  $x_i$  and  $y_j$ , it is possible to find sets of observables  $O_i$  on  $\mathcal{H}$  and  $Q_j$  on  $\mathcal{H}'$  with eigenvalues  $\pm 1$  and  $\dim \mathcal{H} = \dim \mathcal{H}' = n$  such that (B1) holds with  $|\psi\rangle$  a maximally entangled state.

As shown by Wehner [56], this implies that the maximal CHSH value reachable by a quantum system can be calculated using a *semidefinite program* (SDP), more precisely, an optimization problem of the form  $\max: \text{tr}(BG)$ , subject to:  $\text{tr}(E_i G) = e_i$  for all  $i$ , and  $G \succeq 0$ . Here,  $\{E_i, e_i\}_i$  is

a set of linear constraints and  $G$  is the variable to be optimized over (we refer to e.g. [6] for details on semidefinite programming). The reason for this is, that a (real symmetric) matrix  $G$  is positive semidefinite if and only if it can be expressed as  $G = B^\top B$ , i.e., its entries are the inner product of the vectors representing the columns of  $B$ .

For example, for the case of two inputs and outputs, the correlations can be arranged in a  $4 \times 4$  matrix  $G = (g_{ij})$  with  $g_{ij} := x_i^\top \cdot x_j$ . Conversely, any  $4 \times 4$  positive semidefinite matrix with diagonal entries equal to 1 can be seen as an arrangement of this sort, since  $G = B^\top B$  where  $B = (x_1, x_2, y_1, y_2)$ . The expected CHSH value,  $\beta$ , of a certain setup between two parties can be calculated from this matrix  $G$  using

$$\beta(|\psi\rangle, O_1, O_2, Q_1, Q_2) = \langle \psi | O_1 \otimes Q_1 + O_1 \otimes Q_2 + O_2 \otimes Q_1 - O_2 \otimes Q_2 | \psi \rangle = \text{tr}(WG),$$

where  $G$  is defined as above and

$$W := \frac{1}{2} \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \\ 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \end{pmatrix}.$$

## 2. Generalization of Tsirelson's Results

We are here concerned with extending Tsirelson's relation between symmetric matrices and bipartite measurements of the previous section to the case where the overlap of the local observables is restricted. For this purpose, we first define an effective overlap of two observables.

*Definition 4.* Let  $O_1, O_2$  be observables on  $\mathcal{H}$  with binary spectrum  $\{-1, 1\}$  and let  $\rho$  be a density operator acting on  $\mathcal{H}$ . The *effective overlap between the observables  $O_1$  and  $O_2$  on  $\rho$*  is

$$\gamma^*(\rho, O_1, O_2) := \frac{1}{4} \text{tr}(\rho(O_1 + O_2)^2).$$

We will later make a connection between this quantity and the effective overlap of POVMs,  $c^*$ .

The following Lemma is an extension of Tsirelson's [54] original relation in the form used in [56].

**Lemma 8.** *Let  $\rho_{AB}$  be a bipartite quantum state. Furthermore, let  $O_1, O_2, \dots, O_n$  be observables with binary spectrum  $\{-1, 1\}$  on  $A$  and let  $Q_1, Q_2, \dots, Q_m$  be observables with binary spectrum  $\{-1, 1\}$  on  $B$ . Then, there exists a real positive semidefinite  $(n+m) \times (n+m)$  matrix  $G$  such that, for all  $i, i' \in [n], j, j' \in [m]$ ,*

$$\begin{aligned} (G)_{i(n+j)} &= (G)_{(n+j)i} = \text{tr}((O_i \otimes Q_j)\rho_{AB}) \\ (G)_{ii'} &= 2\gamma^*(\rho_A, O_i, O_{i'}) - 1 \\ (G)_{(n+j)(n+j')} &= 2\gamma^*(\rho_B, Q_j, Q_{j'}) - 1 \end{aligned}$$

*Proof.* To prove the statement, we construct the matrix  $G$  for given  $\rho_{AB}$  and observables  $O_i$  and  $Q_j$ . Let  $|\psi\rangle$  be a purification of  $\rho_{AB}$  on an auxiliary system  $C$ . Then, we define vectors for all  $i \in [n], j \in [m]$ :  $x_i := (O_i \otimes \mathbb{1}_B \otimes \mathbb{1}_C)|\psi\rangle$  and  $x_{n+j} := (\mathbb{1}_A \otimes Q_j \otimes \mathbb{1}_C)|\psi\rangle$ . The  $(n+m) \times (n+m)$  matrix  $\bar{G}$  given by the inner products, i.e.  $(\bar{G})_{kk'} = x_k^\dagger x_{k'}$ , is Hermitian and positive semidefinite by construction. Finally,  $G = (\bar{G} + \bar{G}^\top)/2$  is positive semidefinite, real and symmetric.

It remains to check that the correlations agree. First, note that

$$(G)_{i(n+j)} = (\bar{G})_{i(n+j)} = \langle \psi | O_i \otimes Q_j \otimes \mathbb{1}_C | \psi \rangle = \text{tr}((O_i \otimes Q_j)\rho_{AB}).$$

Moreover, the local terms on  $A$  evaluate to

$$\begin{aligned} (G)_{ii'} &= \frac{1}{2} \langle \psi | (O_i O_{i'} \otimes \mathbb{1}_{BC}) | \psi \rangle + \frac{1}{2} \langle \psi | (O_{i'} O_i \otimes \mathbb{1}_{BC}) | \psi \rangle \\ &= \frac{1}{2} \text{tr} (\rho_A (O_i O_{i'} + O_{i'} O_i)) = 2\gamma^*(\rho_A, O_i, O_{i'}) - 1 \end{aligned}$$

and similarly on  $B$  with  $(G)_{(n+j)(n+j)}$ .  $\square$

The converse is also true, for every matrix  $G$  satisfying above properties, there exists a physical realization. This corresponds to the converse of Tsirelson's theorem [54, 55] (see also [57] for a detailed explanation).

**Lemma 9.** *Let  $G$  be a real positive semidefinite  $(n+m) \times (n+m)$  matrix with  $(G)_{ii} = 1$ . Then there exists a quantum state  $\rho_{AB}$ , observables  $O_1, O_2, \dots, O_n$  with binary spectrum  $\{-1, 1\}$  on  $A$  and observables  $Q_1, Q_2, \dots, Q_m$  with binary spectrum  $\{-1, 1\}$  on  $B$ , such that, for all  $i, i' \in [n]$ ,  $j, j' \in [m]$ , it holds that*

$$\begin{aligned} \text{tr} ((O_i \otimes Q_j) \rho_{AB}) &= (G)_{i(n+j)} \\ 2\gamma^*(\rho_A, O_i, O_{i'}) - 1 &= (G)_{ii'} \\ 2\gamma^*(\rho_B, Q_j, Q_{j'}) - 1 &= (G)_{(n+j)(n+j')} \end{aligned}$$

*Proof.* Let  $d = n + m$  and  $\{x_k\}$ ,  $k \in \{1, \dots, d\}$  be a set of real vectors of dimension  $d$  such that  $(G)_{kk'} = x_k^\top x_{k'}$ . Moreover, take  $\rho_{AB} = |\psi\rangle\langle\psi|$ , where  $|\psi\rangle = \sqrt{d}^{-1} \sum_k |k\rangle |k\rangle$  is the maximally entangled state,  $O_i = \sum_\ell (x_i)_\ell \Gamma_\ell^\top$  and  $Q_j = \sum_\ell (x_{n+j})_\ell \Gamma_\ell$  where  $\Gamma_\ell$  are generators of the Clifford algebra in dimension  $n+m$ , i.e.,  $\{\Gamma_\ell, \Gamma_{\ell'}\} = 2\delta_{\ell\ell'} \mathbb{1}$ . Using the fact that  $\Gamma_\ell$  are anti-commuting, it is now straight forward to verify that the  $O_i$  and  $Q_j$  have spectrum in  $\{-1, 1\}$  since

$$O_i O_{i'} = \left( \sum_\ell (x_i)_\ell \Gamma_\ell^\top \right) \left( \sum_{\ell'} (x_{i'})_{\ell'} \Gamma_{\ell'}^\top \right) = \frac{1}{2} \sum_{\ell, \ell'} (x_i)_\ell (x_{i'})_{\ell'} \{\Gamma_\ell, \Gamma_{\ell'}\}^\top = x_i^\top x_{i'} \mathbb{1}.$$

Thus,  $2\gamma^*(\rho_A, Q_i, Q_{i'}) - 1 = \frac{1}{2} \text{tr}(\rho_A \{O_i, O_{i'}\}) = (G)_{ii'}$  and similarly for  $(G)_{(n+j)(n+j')}$ . Finally,

$$\begin{aligned} \langle \psi | O_i \otimes Q_j | \psi \rangle &= \frac{1}{d} \sum_{\ell, \ell'} (x_i)_\ell (x_{n+j})_{\ell'} \left( \sum_{k, k'} \langle k | \langle k | \Gamma_\ell^\top \otimes \Gamma_{\ell'} | k' \rangle | k' \rangle \right) \\ &= \frac{1}{d} \sum_{\ell, \ell'} (x_i)_\ell (x_{n+j})_{\ell'} \text{tr}(\Gamma_\ell \Gamma_{\ell'}) = \sum_{\ell, \ell'} (x_i)_\ell (x_{n+j})_{\ell'} \delta_{\ell\ell'} = (G)_{i(n+j)}. \quad \square \end{aligned}$$

### 3. Two Binary Measurements

Next, we restrict our attention to the case where two parties, Alice and David, each have two observables at their disposal. The measurement setup can in this case be described by the set  $\{|\psi\rangle, O_1, O_2, Q_1, Q_2\}$ . We define the following family of semidefinite programs, which calculate the maximal CHSH value,  $\beta_{\max}(\gamma^*)$ , that can be achieved with a setup for which the effective overlap of Alice's observables satisfies  $\gamma^*(\rho_A, O_1, O_2) = \gamma^*$ . The SDP for  $\beta_{\max}(\gamma^*)$  is given by

$$\begin{aligned} \text{maximize:} \quad & \text{tr}(WG) \\ \text{subject to:} \quad & G \succeq 0, \\ & (G)_{ii} = 1 \quad \forall i \quad \text{and} \\ & (G)_{12} = (G)_{21} = 2\gamma^* - 1. \end{aligned} \tag{B2}$$

Note that, since every physical setup has a corresponding matrix  $G$  due to Lemma 8, the maximization is done over all physical setups that satisfy the constraint on the effective overlap. On the other hand, Lemma 9 tells us that there exists a physical setup—corresponding to the optimal matrix  $G^*$ —that achieves any  $\beta_{\max} = \text{tr}(WG^*)$ . Note, however, that this does not imply that every setup with a given  $\gamma^*$  can be used to reach  $\beta_{\max}(\gamma^*)$ .

The function  $\beta_{\max}(\gamma^*)$  has a nice analytical form, which was conjectured by M. Horodecki [22] for the two qubit case. Alternatively, it is possible to derive a statement of this type [30] using a result of Seevink and Uffink [45], which bounds the maximal CHSH value in terms of the angle between local qubit measurements.

**Lemma 10.** *The maximal CHSH value  $\beta_{\max}$  that can be achieved by a setup  $\{\rho_{AT}, O_1, O_2, Q_1, Q_2\}$  that has a effective overlap  $\gamma^*(\rho_A, O_1, O_2) = \gamma^*$  is given by*

$$\beta_{\max}(\gamma^*) = 2(\sqrt{\gamma^*} + \sqrt{1 - \gamma^*}).$$

*Proof.* The solution is given by the SDP (B2) and it remains to find feasible solutions for both the primal and the dual problem in order to find  $\beta_{\max}$ . We first construct a primal feasible solution  $G^*$  for the SDP (B2). We have,

$$\beta_{\max}(\gamma^*) \geq \text{tr}(WG^*) = 2(\sqrt{\gamma^*} + \sqrt{1 - \gamma^*}), \text{ where}$$

$$G^* := \begin{pmatrix} 1 & 2\gamma^* - 1 & \sqrt{\gamma^*} & \sqrt{1 - \gamma^*} \\ 2\gamma^* - 1 & 1 & \sqrt{\gamma^*} & -\sqrt{1 - \gamma^*} \\ \sqrt{\gamma^*} & \sqrt{\gamma^*} & 1 & 0 \\ \sqrt{1 - \gamma^*} & -\sqrt{1 - \gamma^*} & 0 & 1 \end{pmatrix} \succeq 0, \quad \text{for all } \gamma^* \in [0, 1].$$

To find an upper bound on  $\beta_{\max}$ , we consider the dual SDP, which is

$$\begin{aligned} \text{minimize: } & \Gamma_{11} + \Gamma_{22} + \Gamma_{33} + \Gamma_{44} + (2\gamma^* - 1)(\Gamma_{12} + \Gamma_{21}) \\ \text{subject to: } & \Gamma = \begin{pmatrix} \Gamma_{11} & \Gamma_{12} & 0 & 0 \\ \Gamma_{21} & \Gamma_{22} & 0 & 0 \\ 0 & 0 & \Gamma_{33} & 0 \\ 0 & 0 & 0 & \Gamma_{44} \end{pmatrix} \succeq W. \end{aligned}$$

A feasible solution,  $\Gamma^* \succeq W$ , is

$$\Gamma^* := \begin{pmatrix} \frac{1}{4}\left(\frac{1}{\sqrt{\gamma^*}} + \frac{1}{\sqrt{1-\gamma^*}}\right) & \frac{1}{4}\left(\frac{1}{\sqrt{\gamma^*}} - \frac{1}{\sqrt{1-\gamma^*}}\right) & 0 & 0 \\ \frac{1}{4}\left(\frac{1}{\sqrt{\gamma^*}} - \frac{1}{\sqrt{1-\gamma^*}}\right) & \frac{1}{4}\left(\frac{1}{\sqrt{\gamma^*}} + \frac{1}{\sqrt{1-\gamma^*}}\right) & 0 & 0 \\ 0 & 0 & \sqrt{\gamma^*} & 0 \\ 0 & 0 & 0 & \sqrt{1-\gamma^*} \end{pmatrix},$$

Thus, due to weak duality of semidefinite programming, it holds that  $\beta_{\max}(\gamma^*) \leq \text{tr}(\Gamma^*) + (2\gamma^* - 1)(\Gamma_{12}^* + \Gamma_{21}^*) = 2(\sqrt{\gamma^*} + \sqrt{1 - \gamma^*})$ , which concludes the proof.  $\square$

#### 4. Proof of Theorem 3

We will need a pivotal result due to Jordan [23] (see also [33, 55]).

**Lemma 11** (Jordan's Lemma). *Let  $\mathbf{X} = \{M^0, M^1\}$  and  $\mathbf{Y} = \{N^0, N^1\}$  be two projective measurements with binary outcomes. Then, there exists a projective measurement  $\mathbf{K} = \{P^k\}_k$  that commutes with both  $\mathbf{X}$  and  $\mathbf{Y}$  such that the  $P^k$  project on subspaces of dimension at most 2.*



Let now  $K$  be such a projective measurement for which we additionally require that the rank of the  $P^k$  is minimal. It is easy to verify that this measurement has the property that the projectors  $P^k M^x P^k$  and  $P^k M^y P^k$  either vanish or are rank-1 projectors. (If, for example,  $P^k M^0 P^k$  is not rank-1, it must either be  $P^k$  or vanish. However, this implies that  $P^k M^1 P^k$  also either vanishes or equals  $P^k$  and, thus, measuring further in the basis induced by  $P^k M^y P^k$  will reduce the dimension of  $K$ .) Hence, the projectors can be written in the form  $|\xi_k^x\rangle\langle\xi_k^x| = P^k N^x P^k$  and  $|\zeta_k^y\rangle\langle\zeta_k^y| = P^k N^y P^k$ , where  $|\xi_k^x\rangle$  and  $|\zeta_k^y\rangle$  are allowed to be the zero vector.

It remains to relate the effective overlap of observables,  $\gamma^*$ , to the effective overlap of two POVMs,  $c^*$ . This is done in the following proposition, from which Theorem 3 directly follows.

**Proposition 12.** *For any measurement setup  $\{\rho_A, X, Y\}$ , it holds that*

$$c^*(\rho_A, X, Y) \leq \frac{1}{2} + \frac{\beta}{8} \sqrt{8 - \beta^2}, \quad (\text{B3})$$

where  $\beta = \beta(\rho_{AD}, X, Y, R, S)$  for any extension  $\rho_{AD}$  with  $\rho_A = \text{tr}_D(\rho_{AD})$  and for any two binary POVMs  $R$  and  $S$  on  $D$ .

*Proof.* It is sufficient to consider projective measurements and pure states as, due to Neumark's dilation theorem and the definition of the effective overlap, there exist projective measurements  $X', Y', R', S'$  and an embedded state  $\rho_{A'D'}$  such that

$$\beta(\rho_{AD}, X, Y, R, S) = \beta(\rho_{A'D'}, X', Y', R', S') \quad \text{and} \quad c^*(\rho_A, X, Y) \leq \min_{K'} c_{K'}^*(\rho_{A'}, X', Y'), \quad (\text{B4})$$

where  $K' = \{P_{A'}^k\}_k$  is any projective measurement that commutes with  $X'$  and  $Y'$ .

According to Lemma 11 and (B4), we can thus bound

$$c^*(\rho_A, X, Y) \leq \sum_k \text{tr}(P_{A'}^k \rho_{A'}) \max_x \left\| \sum_y |\zeta_k^y\rangle\langle\zeta_k^y| \xi_k^x \langle\xi_k^x| \zeta_k^y \langle\zeta_k^y| \right\| = \sum_k \text{tr}(P_{A'}^k \rho_{A'}) \max_{x,y} |\langle\xi_k^x|\zeta_k^y\rangle|^2, \quad (\text{B5})$$

where  $P_{A'}^k$  is a decomposition into at most two-dimensional subspaces,  $|\xi_k^x\rangle\langle\xi_k^x| = P_{A'}^k M_{A'}^x P_{A'}^k$ , and  $|\zeta_k^y\rangle\langle\zeta_k^y| = P_{A'}^k N_{A'}^y P_{A'}^k$ . Now, consider the observables

$$\tilde{O}_{A'}^X = \bigoplus_k \left( |\xi_k^{x_k}\rangle\langle\xi_k^{x_k}| - |\xi_k^{\bar{x}_k}\rangle\langle\xi_k^{\bar{x}_k}| \right) \quad \text{and} \quad \tilde{O}_{A'}^Y = \bigoplus_k \left( |\zeta_k^{y_k}\rangle\langle\zeta_k^{y_k}| - |\zeta_k^{\bar{y}_k}\rangle\langle\zeta_k^{\bar{y}_k}| \right),$$

where  $x_k, y_k \in \{0, 1\}$  are the values that maximize the overlap in (B5) for each value of  $k$ . Furthermore,  $\bar{x}_k = 1 - x_k$  and  $\bar{y}_k = 1 - y_k$ . Using these observables, it is easy to verify that

$$\sum_k \text{tr}(P_{A'}^k \rho_{A'}) \max_{x,y} |\langle\xi_k^x|\zeta_k^y\rangle|^2 = \gamma^*(\rho_{A'}, \tilde{O}_{A'}^X, \tilde{O}_{A'}^Y) = \frac{1}{2} + \frac{\beta_{\max}(\gamma^*)}{8} \sqrt{8 - \beta_{\max}(\gamma^*)^2},$$

where, in the last step, we used Lemma 10 and introduce  $\beta_{\max}(\gamma^*)$ , the maximum CHSH value that can be reached with a bipartite setup that satisfies  $\gamma^*(\rho_{A'}, \tilde{O}_{A'}^X, \tilde{O}_{A'}^Y) = \gamma^*$ .

It remains to show that  $\beta(\rho_{A'D}, X', Y', R', S') \leq \beta_{\max}(\gamma^*)$ . First note that due to the fact that  $K'$  commutes with  $X'$  and  $Y'$ , we have  $\beta(\rho_{A'D}, X', Y', R', S') = \beta(\rho_{A'DK}, X', Y', R', S')$  where  $\rho_{A'DK} = \sum_k |k\rangle\langle k| \otimes P_{A'}^k \rho_{A'D} P_{A'}^k$ . Thus, we can assume without loss of generality that the maximum CHSH value is achieved with an extension and measurements that potentially depend on the value of  $K$ . Furthermore, we introduce a purification  $|\psi\rangle$  of  $\rho_{A'DK}$  and write

$$\begin{aligned} \beta(\rho_{A'D}, X', Y', R', S') &\leq \max_{|\psi\rangle, Q_{D'}^R, Q_{D'}^S} \beta(|\psi\rangle, O_{A'}^X, O_{A'}^Y, Q_{D'}^R, Q_{D'}^S) \\ &= \max_{|\psi\rangle, Q_{D'}^R, Q_{D'}^S} \beta(|\psi\rangle, \tilde{O}_{A'}^X, \tilde{O}_{A'}^Y, Q_{D'K}^R, Q_{D'K}^S) \leq \beta_{\max}(\gamma^*), \end{aligned} \quad (\text{B6})$$

where the measurements  $X$  and  $Y$  are represented as observables

$$O_{A'}^X = M_{A'}^0 - M_{A'}^1 = \bigoplus_k \left( |\xi_k^0\rangle\langle\xi_k^0| - |\xi_k^1\rangle\langle\xi_k^1| \right) \quad \text{and} \quad O_{A'}^Y = N_{A'}^0 - N_{A'}^1 = \bigoplus_k \left( |\zeta_k^0\rangle\langle\zeta_k^0| - |\zeta_k^1\rangle\langle\zeta_k^1| \right).$$

The equality in (B6) requires some explanation. Note that the observables  $O$  and  $\tilde{O}$  only differ in the way outputs, 0 or 1, are labelled for each  $k$ . However, due to the symmetry of the CHSH value, it is easy to verify that David can simulate a  $k$ -dependent relabeling of Alice's outputs by permuting his inputs and outputs. More precisely, we have

$$\beta(|\psi\rangle, O_{A'}^X, O_{A'}^Y, Q_{D'}^R, Q_{D'}^S) = \beta(|\psi\rangle, \tilde{O}_{A'}^X, \tilde{O}_{A'}^Y, Q_{D'K}^R, Q_{D'K}^S)$$

for the observables  $Q_{D'K}^R = \sum_k |k\rangle\langle k| \otimes Q_{D'}^{R,k}$  and  $Q_{D'K}^S = \sum_k |k\rangle\langle k| \otimes Q_{D'}^{S,k}$ , where

$$\{Q_{D'}^{R,k}, Q_{D'}^{S,k}\} = (-1)^{x_k} \begin{cases} \{Q_{D'}^R, Q_{D'}^S\} & \text{if } x_k \oplus y_k = 0 \\ \{Q_{D'}^S, Q_{D'}^R\} & \text{if } x_k \oplus y_k = 1 \end{cases}.$$

The last inequality in (B6) follows by definition of  $\beta_{\max}(\gamma^*)$  and concludes the proof.  $\square$