The Link between Uncertainty Relations and Non-Locality

Esther Hänggi
Centre for Quantum Technologies, National University of Singapore, Singapore

Marco Tomamichel
Institute for Theoretical Physics, ETH Zurich, 8093 Zurich, Switzerland
(Dated: November 9, 2011)

Two of the most intriguing features of quantum physics are the *uncertainty principle* and the occurrence of *non-local correlations*. The uncertainty principle states that there exist pairs of non-compatible measurements on quantum systems such that their outcomes cannot be simultaneously predicted by any observer. Non-local correlations of measurement outcomes at different locations cannot be explained by classical physics, but appear in quantum mechanics in the presence of entanglement. Here, we show that these two essential properties of quantum mechanics are quantitatively related. Namely, we provide an entropic uncertainty relation that gives a lower bound on the uncertainty of the binary outcomes of two measurements in terms of the maximum Clauser-Horne-Shimony-Holt value that can be achieved using the same measurements. We discuss an application of this uncertainty relation to certify a quantum source using untrusted devices.

A technical version is available at `http://arxiv.org/abs/1108.5349` [1].

A remarkable property of quantum physics is the *uncertainty principle*, as first described by Heisenberg [2] and Robertson [3], namely the fact that there exist certain observable properties of a quantum system such that knowledge of one necessarily implies uncertainty about the other. Recent uncertainty relations are often formulated in terms of entropies [4–11]. These relations give lower bounds on the uncertainty — quantified by entropies — of the measurement outcomes of two or more incompatible measurements. (See [12] for a recent review.)

Entropic uncertainty relations have been extended to include the case when observers have access to a quantum system that is correlated with the state prior to measurement [7]. There, the principle is formulated in terms of conditional von Neumann entropies $H(A|B)_\rho := H(\rho_{AB}) - H(\rho_B)$. They consider a tripartite quantum system shared between Alice (A), Bob (B) and Charlie (C) that is prepared in an arbitrary joint state ρ_{ABC}. Alice then measures her system in either one of two bases, $\{|x\rangle\}$ or $\{|y\rangle\}$. This measurement results in the post-measurement state ρ_{XBC} or ρ_{YBC}, respectively, where X and Y are registers containing the measurement result. The uncertainty relation of [7] reads

$$H(X|B) + H(Y|C) \geq -\log_2 c\,, \tag{1}$$

where $c = \max_{x,y} |\langle x|y\rangle|^2$ is the maximal *overlap* of the eigenvectors of the two measurements and is independent of the state ρ_{ABC} before measurement. Hence, Eq. (1) gives a non-trivial lower bound on the uncertainty that two observers, Bob and Charlie, have about the outcomes of two measurements whenever these measurements have an overlap $c < 1$. For example, if Bob can predict the outcome of the X measurement with certainty (this corresponds to $H(X|B) = 0$), then Charlie necessarily has uncertainty about the outcome of the Y measurement (i.e., $H(Y|C) > 0$). The relation (1) has been further generalized to include arbitrary positive operator-valued measurements (POVMs) in [8] and [11].

Entropic uncertainty relations do not only describe a fundamental property of quantum physics, they have also found applications in the context of entanglement witnesses [7], information locking [13] and quantum cryptography [10, 14–16]. Intuitively, their usefulness can be explained by the fact that the entropies on the l.h.s. of (1) characterize operational quantities in information theory, e.g. the asymptotic data compression rate with quantum side information [17].

Many recent entropic uncertainty relations [7–9, 11] give a bound on the uncertainty in terms of the overlap c which is a function of the two measurements (more precisely, their POVM elements) but not of the state of Alice's system prior to the measurement. This is often desirable, since it leads to a very general uncertainty relation which holds for *all* possible states. However, because of this generality, the resulting uncertainty relation can sometimes be unnecessarily weak. We will see that in some situations partial knowledge about the state before measurement can be used to improve the bound on the uncertainty.

Our first result is thus a generalized uncertainty relation of the form (1) that introduces a trade-off between information about the state before measurement and tightness of the uncertainty relation. Specifically, we consider the *effective overlap* of a measurement setup, denoted by c^*, which describes the overlap of the two measurements on Alice's marginal state.

Result 1.

$$H(X|B) + H(Y|C) \geq -\log_2 c^*\,. \tag{2}$$

We refer to [1] for a precise definition of c^*, but, as an example, consider the scenario where we apply one of two projective measurements, either in the basis $\{|0\rangle, |1\rangle, |\perp\rangle\}$ or $\{|+\rangle, |-\rangle, |\perp\rangle\}$ on a state ρ which has the property that '$\perp$' is measured with probability at most ε. Our

intuitive understanding of this situation tells us that the uncertainty about the measurement outcome is high as long as ε is small. However, applying the 'traditional' state-independent uncertainty relation (1) to this setup will only lead to a trivial result, since $c = 1$. The effective overlap, on the other hand, satisfies $c^* \leq (1-\varepsilon)\frac{1}{2}+\varepsilon$. (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 ε we measure $\perp$ and have full overlap.) Thus, the total entropic uncertainty is nonzero as long as $\varepsilon < 1$ and approaches the maximum value of 1 when ε is close to zero.

Besides uncertainty relations, another phenomenon distinguishing quantum from classical physics is the occurrence of *non-local correlations*. It has already been observed by Einstein, Podolsky and Rosen [18] that quantum mechanics predicts correlations between entangled, but spatially separated particles. Bell [19] later showed that certain of these correlations cannot be explained by a local hidden-variable theory, i.e., they are non-local. Non-locality can be quantified using so-called Bell inequalities [19, 20]. The best-known Bell inequality, the CHSH inequality [20], considers the case of a bipartite system, shared between Alice and Thomas (T), to which each party applies one out of two possible measurements with binary outcomes. We denote the outcomes of Alice's measurements X and Y (as in the setup of the uncertainty relation) and Thomas' outcomes by R and S, depending on his choice of measurement. The CHSH inequality states that for any such system which can be described by a local hidden-variable theory, it holds that $\beta \leq 2$, where

$$\beta := 2\big(\Pr[X{=}R]+\Pr[Y{=}R]+\Pr[X{=}S]-\Pr[Y{=}S]-1\big)$$

is called the CHSH value. If $\beta > 2$, we call the correlations between Alice and Thomas non-local, and quantum mechanics allows correlations that achieve $\beta = 2\sqrt{2}$.

Our second result shows that there is a close relation between the effective overlap of two measurements with binary outcomes on Alice's system and the CHSH value, β, that can be reached between Alice and Thomas, when the same setup is used on Alice's system.[1] (Note that Thomas could, in particular, be part of Bob's or Charlie's system.) We show that any measurement setup by Alice which can give rise to non-local correlations (i.e., $\beta > 2$), must have overlap $c^* < 1$. Furthermore, in order to reach a CHSH value close to the maximum quantum value (i.e., $\beta \approx 2\sqrt{2}$), Alice's setup must have almost minimal overlap $c^* \approx 1/2$.

Result 2. *The CHSH value that can be reached between Alice and Thomas when the effective overlap of Alice's setup is c^* is bounded by*

$$\beta(c^*) \leq 2\big(\sqrt{c^*} + \sqrt{1-c^*}\big) \,. \tag{3}$$

Conversely, given a CHSH value β between Alice and Thomas, the effective overlap of Alice's measurement setup is bounded by

$$c^* \leq \frac{1}{2} + \frac{\beta}{8}\sqrt{8-\beta^2} \,.$$

This relation is depicted in Figure 1. Note that for the case when the systems A and T are restricted to qubits, a bound on the maximal CHSH value in terms of the angle between local qubit measurements has previously been derived by Seevink and Uffink [22]. The relation between uncertainty and non-locality has been conjectured in [23] and independently derived in [24] for the case of qubit-systems.

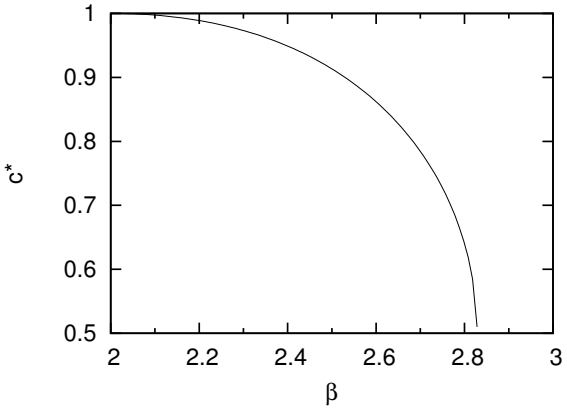

FIG. 1. The relation between overlap and CHSH value. Due to our bound (3), combinations of β and c^* above the curve are impossible.

The above relation implies that the overlap of a setup can be tested by looking at the Bell inequality violation it reaches with a second system. Together with the first result, it leads to an uncertainty relation with quantum side-information in terms of the violation of a Bell inequality this system can reach. This device-independent uncertainty relation is stated only in terms of quantities which have an operational meaning.

Result 3.

$$H(X|B)_\rho + H(Y|C)_\rho \geq 1 - f(\beta) \,, \tag{4}$$

where $f(\beta) = \log_2\big(1 + \frac{\beta}{4}\sqrt{8-\beta^2}\big)$ and β is the CHSH value between Alice and Thomas.

Note that in order to determine the value of the overlap c used in previous uncertainty relations, and, therefore, a meaningful uncertainty relation of the form (1), one usually needs to know the exact specification of the Alice's measurement devices. In contrast to this, our uncertainty

[1] Oppenheim and Wehner [21] showed that the uncertainty, via steering, directly determines the strength of achievable non-locality. Our result is complementary to theirs, as we show that in order to achieve a certain non-locality, at least some specific amount of uncertainty is necessary.

relations depends *only* on the Bell value and is independent of the details of the physical model used to describe the quantum systems and measurements. This includes, in particular, the dimension of the Hilbert space they act on (although we do assume that it is finite).

The uncertainty relation in terms of the violation of a Bell inequality, Eq. (4), can be used to certify the quality of a source of BB84-states using an untrusted certification device. Sources of BB84-states are widely used in quantum cryptography [25], including quantum key distribution [26, 27], and bit commitment or oblivious transfer secure in the bounded/noisy storage model [16, 28].

For our application, consider a (potentially imperfect) source that creates these states in the following way. First, it produces two entangled particles, e.g. through parametric down-conversion [29, 30]. Then, it sends one part out and measures the other part, using either one of two different measurements at random and taking note of the measurement outcome (see Figure 2). 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. (This technique of remotely preparing states by means of entanglement is often referred to as steering.) We assume that the source prepares the same state and uses the same measurements in each run — in particular, this means that the source is memoryless. Sources of this type are the subject of recent research, e.g. they are used as heralded single-photon sources [31, 32] and have applications in (device-independent) quantum cryptography [33–35].

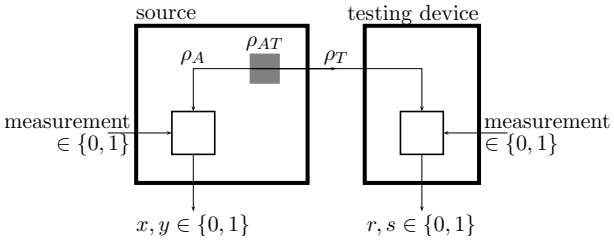

FIG. 2. Source testing.

Uncertainty relations of the form (1) and (2) lie at the core of security proofs in quantum cryptography. These include cryptography in the bounded quantum storage model [16], oblivious transfer and bit commitment in the noisy quantum storage model [28] and recent security proofs for quantum key distribution [7, 11, 15]. For example, in the case of key distribution the overlap of the source enters as a crucial parameter determining the secrecy of the resulting key [11, 15]. Moreover, it sufficiently characterizes the source for the purpose of these security proofs as long as the source is of the type described above. In particular, it is unnecessary to do tomography of the states the source produces. We, therefore, propose the effective overlap c^* as the parameter to quantify the quality of sources of BB84-states.

Our results imply that the effective overlap can be tested using a certification device (Thomas, in the above discussions) which, using a random bit and the state sent by the source as input, tries to output a bit in such a way that the CHSH-condition (i.e., either $x = r$, $x = s$, $y = r$ or $y \neq s$) is fulfilled (see Figure 2). Our analysis shows that the effective overlap of the source can now be estimated from the fraction of times, p, the CHSH-condition is satisfied. That is, except with very small probability, it holds that

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

Since the test verifies this property of the apparatus independently of the physical implementation of the certification device, we believe that this test could be useful to manufacturers of quantum cryptographic devices who would like to prove — to a skeptical audience that may not trust the certification device — whether their devices fulfill the desired specifications.

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

[1] E. Hänggi and M. Tomamichel(2011), `http://arxiv.org/abs/1108.5349`.
[2] W. Heisenberg, Zeitschrift für Physik **43**, 172 (1927).
[3] H. P. Robertson, Phys. Rev. **34**, 163 (1929).
[4] D. Deutsch, Phys. Rev. Lett. **50**, 631 (1983).
[5] H. Maassen and J. B. M. Uffink, Phys. Rev. Lett. **60**, 1103 (1988).
[6] M. Krishna and K. R. Parthasarathy, Ind. J. Stat. **64**, 842 (2001).
[7] M. Berta, M. Christandl, R. Colbeck, J. M. Renes, and R. Renner, Nat. Phys. **6**, 659 (2010).
[8] P. J. Coles, L. Yu, V. Gheorghiu, and R. B. Griffiths(2010), `http://arxiv.org/abs/1006.4859`.
[9] P. J. Coles, L. Yu, and M. Zwolak(2011), `http://arxiv.org/abs/1105.4865`.
[10] I. B. Damgård, S. Fehr, R. Renner, L. Salvail, and C. Schaffner, in *CRYPTO'07* (2007) pp. 360–378.
[11] M. Tomamichel and R. Renner, Phys. Rev. Lett. **106**, 110506 (2011).
[12] S. Wehner and A. Winter, New J. Phys. **12**, 025009 (2010).
[13] M. Christandl and A. Winter **51**, 3159 (2005).
[14] M. Koashi, J. Phys. **36**, 98 (2006).
[15] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner(2011), `http://arxiv.org/abs/1103.4130`.

[16] I. Damgård, S. Fehr, L. Salvail, and C. Schaffner, in *FOCS'05* (2005) pp. 449–458.
[17] I. Devetak and A. Winter, Phys. Rev. A **68**, 1 (2003).
[18] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).
[19] J. S. Bell, Physics **1**, 195 (1964).
[20] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).
[21] J. Oppenheim and S. Wehner, Science **330**, 1072 (2010).
[22] M. Seevinck and J. Uffink, Phys. Rev. A **76**, 1 (2007).
[23] M. Horodecki, Personal communication (2011).
[24] C. C. W. Lim *et al.*, Manuscript in Preparation (2011).
[25] S. Wiesner, SIGACT News **15**, 78 (1983).
[26] C. H. Bennett and G. Brassard, in *Proc. IEEE Int. Conf. Comp., Syst. and Sig. Proc.* (1984).
[27] N. J. Bouman and S. Fehr, in *CRYPTO'10* (2010) pp. 724–741.
[28] R. König, S. Wehner, and J. Wullschleger(2009), `http://arxiv.org/abs/0906.1030`.
[29] Y. Shih and C. O. Alley, Phys. Rev. Lett. **61**, 2921 (1988).
[30] T. E. Kiess, Y. Shih, A. V. Sergienko, and C. O. Alley, Phys. Rev. Lett. **71**, 3893 (1993).
[31] T. Pittman, B. Jacobs, and J. Franson, Opt. Comm. **246**, 545 (2005).
[32] G. Y. Xiang, T. C. Ralph, A. P. Lund, N. Walk, and G. J. Pryde, Nat. Phot. **4**, 316 (2010).
[33] N. Gisin, S. Pironio, and N. Sangouard, Phys. Rev. Lett. **105**, 5 (2010).
[34] M. Curty and T. Moroder, Phys. Rev. A **84**, 010304 (2011).
[35] D. Pitkänen, X. Ma, R. Wickert, P. van Loock, and N. Lütkenhaus(2011), `http://arxiv.org/abs/1105.2811`.