Device-independent uncertainty for binary observables

Jędrzej Kaniewski,* Marco Tomamichel, and Stephanie Wehner
Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543

We investigate entropic uncertainty relations for two or more binary measurements. We show that the effective anti-commutator is a useful measure of incompatibility and gives rise to strong uncertainty relations. Since the effective anti-commutator can be certified device-independently it leads us to *device-independent uncertainty*. Our relations, expressed in terms of conditional Rényi entropies, turn out to be robust (they give non-trivial bounds on the uncertainty whenever deterministic behaviour cannot be ruled out) and strong (e.g. for the well-studied case of two projective measurements on a qubit we find an analytic expression that improves on the celebrated bound due to Maassen and Uffink [Phys. Rev. Lett. **60**, 1103 (1988)] and some recent bounds based on the majorisation approach). In addition to being a useful tool towards robust, device-independent quantum cryptography beyond quantum key distribution (QKD), our results are also interesting from the technical point of view since the methods used rely solely on standard matrix analysis and differ substantially from the techniques usually employed in deriving uncertainty relations.

Full version available at `arXiv: 1402.5722`

I. SUMMARY OF RESULTS

In the device-independent scenario, the honest parties are required to perform a certain task using devices whose internal working is not specified (in the worst case scenario they have been supplied by an adversary) [ABG+07, PAB+09]. Therefore, the cryptographic protocol must be supplemented by some tests to convince ourselves that the device behaves as expected. This is closely related to the concept of self-testing [MY98, MY04, MM11].

In most cryptographic protocols proving security amounts to showing that there is a secret that the dishonest party is ignorant about, or, alternatively, that the *uncertainty* of the secret given his knowledge is high. It is clear that uncertainty relations might come in useful in proving such statements and, indeed, they constitute an important ingredient of many security proofs. Unfortunately, no uncertainty relation can be stated if we do not know what the device is actually doing. In fact, most standard uncertainty relations are stated under the assumption that we know the *exact* specification of the device.

To overcome this issue we need to develop uncertainty relations that do not require the exact specification of the device and rely only on simple properties which can be verified experimentally. This is the essence of *device-independent uncertainty*. This approach has been successful in proving security of quantum key distribution [VV14, LPT+13] and randomness expansion [VV12, MS14].

The goal of current work is to develop a robust framework for device-independent uncertainty. While the case of two measurements has received significant attention essentially nothing is known beyond that. Our findings strengthen the existing results for two measurements and derive novel, device-independent uncertainty relations for more than two measurements. For simplicity we consider measurements with two outcomes. These have an equivalent description as binary observables, i.e. Hermitian operators whose eigenvalues are ± 1 (assuming the measurements are projective; our techniques also apply to generalised observables, please refer to the full paper for details). It is known that for binary observables anti-commutation (in the operator sense) implies incompatibility and gives rise to strong uncertainty relations (e.g. σ_x and σ_z are the most incompatible binary measurements on a qubit). While the case of perfect anti-commutation is well understood [WW08] nothing is known about the case of partial (or approximate) anti-commutation. Since for most applications we need uncertainty relations which are robust against small perturbations we turn to study observables which only partially anti-commute as quantified by their pairwise *effective anti-commutator*. Effective anti-commutators turn out to be appealing objects to study since they can be certified in a device-independent fashion [TH13, LPT+13].

* j.kaniewski@nus.edu.sg

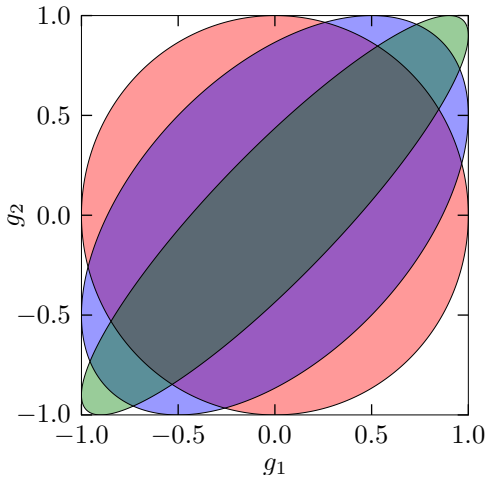

Fig. 1: The allowed expectation values of two observables with a fixed effective anti-commutator, $\varepsilon \in \{0, 0.5, 0.9\}$.

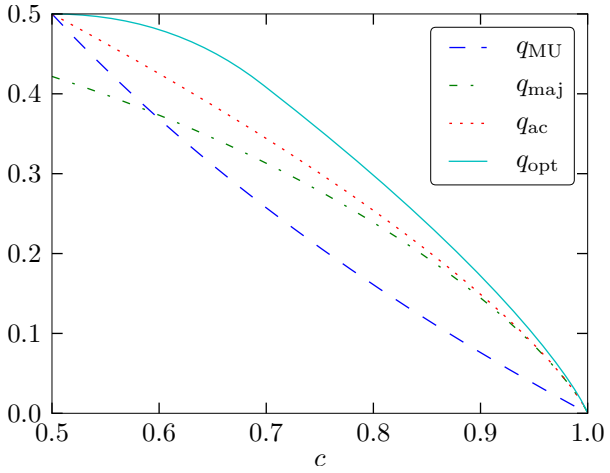

Fig. 2: Various lower bounds on $H(A|K)$ as a function of the overlap, c (q_{MU} : Maassen-Uffink, q_{maj} : majorisation bound, q_{ac} : anti-commutation bound, q_{opt} : largest, state-independent bound; details in the text).

In our work we propose a procedure that allows to quantify uncertainty generated by an untrusted device. In our setting we are given two devices: the primary device, whose uncertainty we want to certify, and an auxiliary device which will be used for testing purposes only. We assume that both devices are memoryless. The procedure is as follows.

1. We use the devices to play a non-local game proposed by Slofstra [Slo11].
2. From the observed statistics using the main result of [TH13, LPT+13] we derive bounds on the effective anti-commutators of the measurements performed by the primary device.
3. We show that bounds on the effective anti-commutators imply lower bounds on the entropic uncertainty of these observables (our contribution).

Our contribution is a stepping stone towards robust device-independent security proofs and we hope it will find numerous applications in quantum cryptography. For example the techniques used for proving security of QKD cannot be directly applied to the problem of device-independent two-party cryptography (in the bounded [DFSS05, DFR+07] or noisy [WST08, KWW12] storage model). However, the success of uncertainty-based techniques in QKD suggests that device-independent uncertainty might also be useful in the two-party scenario.

We believe our results are of interest to the quantum cryptography community for several reasons. First of all, the problem and final results are simple to state and understand (in particular, multiple parts of the proof and the solution admit a simple geometrical interpretation, see Section II for an example). Our results are robust which means they give a lower bound on the uncertainty for an arbitrary set of binary measurements and the lower bound is strictly positive whenever any Bell violation is observed. (Note that this is the best one can hope for since if no violation is observed, the statistics can be reproduced by local hidden variables and, hence, no uncertainty can be guaranteed.) Moreover, our bounds are strong: for the case of two projective measurements on a qubit we provide an analytic expression that outperforms the celebrated bound due to Maassen and Uffink [MU88] and some recent bounds based on the majorisation approach [FGG13, PRŻ13] (and more recently [RPŻ14]). See Section II for an explicit comparison. Last but not least, our uncertainty bounds can be stated in a closed-form and are simple to evaluate (in particular, no numerical optimisation is required).

From the technical point of view our proof is concise and accessible since it only relies on standard tools from matrix analysis. Moreover, since we do not rely on Jordan's lemma (which leads to a reduction to qubits but only applies to two measurements), we can treat any (finite) number of observables. For a meaningful comparison we must, however, restrict ourselves to the well-studied case of two measurements since very few results are known beyond that.

II. EXAMPLE: UNCERTAINTY FOR TWO MEASUREMENTS

Consider two binary observables denoted by A_0 and A_1 (whose outcomes are labelled by ± 1) and suppose that our system is in the state ρ. The effective anti-commutator of these observables equals $\varepsilon = \frac{1}{2}\operatorname{tr}(\{A_0, A_1\}\rho)$, where $\{A_0, A_1\} = A_0A_1 + A_1A_0$ is the anti-commutator. The effective anti-commutator is a real number and $|\varepsilon| \leq 1$. We expect small effective anti-commutator (in modulus) to be a signature of incompatibility (e.g. for σ_x and σ_z we have $\varepsilon = 0$ independent of the state). We prove that this is indeed the case by showing that the effective anti-commutator imposes a constraint on the probability distributions of the observables. Let $g_k = \operatorname{tr}(A_k\rho)$ be the expectation value of A_k (note that for two outcomes the expectation value determines the distribution uniquely: e.g. $g_k = 0$ corresponds to the uniform distribution, while $g_k = \pm 1$ corresponds to a deterministic one) and define the (column) vector of expectation values $g = (g_1, g_2)$. We show that if the effective anti-commutator equals ε then g must satisfy

$$gg^{\mathrm{T}} \leq \begin{pmatrix} 1 & \varepsilon \\ \varepsilon & 1 \end{pmatrix},$$

which geometrically corresponds to lying inside an ellipse as shown in Fig. 1. For $\varepsilon = 0$ we obtain a circle, which becomes gradually elongated towards the corners as ε increases. Note that $\varepsilon > 0$ ($\varepsilon < 0$) encourages the two expectation values to be correlated (anti-correlated), which results in an ellipse stretched along the primary (secondary) diagonal. The deterministic points, corresponding to the corners, are only allowed for $|\varepsilon| = 1$. Note that this neat result generalises to the case of multiple observables: the vector of expectation values of M measurements must lie inside an M-dimensional ellipsoid specified by the pairwise anti-commutators.

To obtain uncertainty in terms of entropies one needs to minimise the entropy of choice over the ellipse. While solving the optimisation problem exactly might be difficult it is possible to obtain bounds (which turn out to be quite strong). As an example suppose we want to obtain a bound q on the average of the Shannon entropies of the two measurements (which is equivalent to the conditional Shannon entropy), $H(A|K) = \frac{1}{2}(H(A_0) + H(A_1)) \geq q$. Our approach gives

$$q_{ac}(\varepsilon) = \frac{1}{2}h\left(\frac{1 + \sqrt{|\varepsilon|}}{2}\right),$$

where $h(p) = -p\log p - (1-p)\log(1-p)$ is the binary entropy. Although effective anti-commutators play a central role in our work, it is more common to state uncertainty relations in terms of the overlap, which for rank-1 projective measurements corresponding to orthogonal bases $\{|x_j\rangle\}$ and $\{|y_j\rangle\}$ equals $c = \max_{jk} |\langle x_j | y_k\rangle|^2$. In general the relationship between the two is non-trivial but for rank-1 projective measurements on a qubit we have $c = (1 + |\varepsilon|)/2$ which allows to rewrite our bound as a function of the overlap

$$q_{\mathrm{ac}}(c) = \frac{1}{2}h\left(\frac{1 + \sqrt{2c-1}}{2}\right).$$

Now, we can compare it with the Maassen-Uffink and majorisation bounds:

$$q_{\mathrm{MU}}(c) = -\frac{1}{2}\log c,$$

$$q_{\mathrm{maj}}(c) = \frac{1}{2}h\left(\frac{\left(1 + \sqrt{c}\right)^2}{4}\right).$$

For comparison Fig. 2 also shows the largest state-independent lower bound denoted by $q_{\mathrm{opt}}(c)$ (for $c \gtrsim 0.7$ we have an analytic expression due to Ghirardi et al. [GMR03], while for $c \lesssim 0.7$ one needs to resort to numerics).

[ABG+07] 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): 230501, 2007. DOI: 10.1103/PhysRevLett.98.230501.

[DFR+07] I. B. Damgård, S. Fehr, R. Renner, L. Salvail, and C. Schaffner. A Tight High-Order Entropic Quantum Uncertainty Relation with Applications. *Proc. 27th CRYPTO*, pages 360–378, 2007.
DOI: 10.1007/978-3-540-74143-5_20.

[DFSS05] I. B. Damgård, S. Fehr, L. Salvail, and C. Schaffner. Cryptography In the Bounded Quantum-Storage Model. *Proc. 46th IEEE FOCS*, pages 449 – 458, 2005.
DOI: 10.1109/SFCS.2005.30.

[FGG13] S. Friedland, V. Gheorghiu, and G. Gour. Universal Uncertainty Relations. *Phys. Rev. Lett.*, 111(23): 230401, 2013.
DOI: 10.1103/PhysRevLett.111.230401.

[GMR03] G. Ghirardi, L. Marinatto, and R. Romano. An optimal entropic uncertainty relation in a two-dimensional Hilbert space. *Phys. Lett. A*, 317(1-2): 32–36, 2003.
DOI: 10.1016/j.physleta.2003.08.029.

[KWW12] R. König, S. Wehner, and J. Wullschleger. Unconditional Security From Noisy Quantum Storage. *IEEE Trans. Inf. Theory*, 58(3): 1962–1984, 2012.
DOI: 10.1109/TIT.2011.2177772.

[LPT+13] C. C. W. Lim, C. Portmann, M. Tomamichel, R. Renner, and N. Gisin. Device-Independent Quantum Key Distribution with Local Bell Test. *Phys. Rev. X*, 3(3): 031006, 2013.
DOI: 10.1103/PhysRevX.3.031006.

[MM11] M. McKague and M. Mosca. Generalized Self-testing and the Security of the 6-State Protocol. *Proc. 5th TQC*, pages 113–130, 2011.
DOI: 10.1007/978-3-642-18073-6_10.

[MS14] C. A. Miller and Y. Shi. Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices. 2014.
arXiv: 1402.0489.

[MU88] H. Maassen and J. B. M. Uffink. Generalized Entropic Uncertainty Relations. *Phys. Rev. Lett.*, 60(12): 1103–1106, 1988.
DOI: 10.1103/PhysRevLett.60.1103.

[MY98] D. Mayers and A. Yao. Quantum cryptography with imperfect apparatus. *Proc. 39th IEEE FOCS*, pages 503–509, 1998.
DOI: 10.1109/SFCS.1998.743501.

[MY04] D. Mayers and A. Yao. Self testing quantum apparatus. *Quant. Inf. Comp.*, 4(4): 273–286, 2004.
Online: http://www.rintonpress.com/xqic4/qic-4-4/273-286.pdf.

[PAB+09] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani. Device-independent quantum key distribution secure against collective attacks. *New J. Phys.*, 11(4): 045021, 2009.
DOI: 10.1088/1367-2630/11/4/045021.

[PRŻ13] Z. Puchała, Ł. Rudnicki, and K. Życzkowski. Majorization entropic uncertainty relations. *J. Phys. A*, 46(27): 272002, 2013.
DOI: 10.1088/1751-8113/46/27/272002.

[RPŻ14] Ł. Rudnicki, Z. Puchała, and K. Życzkowski. Strong Majorization Entropic Uncertainty Relations. 2014.
arXiv: 1402.0129.

[Slo11] W. Slofstra. Lower bounds on the entanglement needed to play XOR non-local games. *J. Math. Phys.*, 52(10): 102202, 2011.
DOI: 10.1063/1.3652924.

[TH13] M. Tomamichel and E. Hänggi. The link between entropic uncertainty and nonlocality. *J. Phys. A*, 46(5): 055301, 2013.
DOI: 10.1088/1751-8113/46/5/055301.

[VV12] U. Vazirani and T. Vidick. Certifiable quantum dice: or, true random number generation secure against quantum adversaries. *Proc. 44th ACM STOC*, pages 61–76, 2012.
DOI: 10.1145/2213977.2213984.

[VV14] U. Vazirani and T. Vidick. Fully device independent quantum key distribution. *Proc. 5th ITCS*, pages 35–36, 2014.
DOI: 10.1145/2554797.2554802.

[WST08] S. Wehner, C. Schaffner, and B. Terhal. Cryptography from Noisy Storage. *Phys. Rev. Lett.*, 100(22): 220502, 2008.
DOI: 10.1103/PhysRevLett.100.220502.

[WW08] S. Wehner and A. Winter. Higher entropic uncertainty relations for anti-commuting observables. *J. Math. Phys.*, 49(6): 062105, 2008.
DOI: 10.1063/1.2943685.