OPERATIONALLY-MOTIVATED HEISENBERG UNCERTAINTY RELATIONS

JOSEPH M. RENES AND VOLKHER B. SCHOLZ

Abstract. Heisenberg's original formulation of the uncertainty principle, forbidding error-free measurement of one observable without disturbance to noncommuting observables, remains a cornerstone of our understanding of quantum mechanics [Z. Phys. 43, 172–198 (1927)]. Recently there has been an increased interest in and dispute regarding uncertainty relations which formalize this principle, as well as appropriate means of defining measurement error and disturbance. Here we introduce clear and unambiguous measures of error and disturbance in terms of a directly operational quantity, the probability of distinguishing the actual operation of a device from its hypothetical ideal by any possible testing procedure. We then establish uncertainty relations for both the joint measurability of two arbitrary observables and their error-disturbance tradeoff. Our relations may be directly applied in information processing settings, for example to infer that devices which can faithfully transmit information regarding one observable do not leak any information whatsoever about conjugate observables to the environment.

Full Paper: arXiv:1402.6711

Heisenberg mentions two facets to the uncertainty principle in his original 1927 formulation. The first restricts the joint measurability of observables, stating that noncommuting observables can only be simultaneously determined with a characteristic amount of indeterminacy [6, p. 172]. The second describes an error-disturbance tradeoff, noting that the more precise a measurement of one observable is made, the greater the disturbance to noncommuting observables [6, p. 175].

Precise formal statements corresponding to these two notions were constructed only much later, due to the lack of precise mathematical descriptions of the measurement process in quantum mechanics. Here we must be careful to draw a distinction between statements addressing Heisenberg's original notions of uncertainty from those, like the standard Robertson uncertainty relation [13], which address the impossibility of finding a quantum state with well-defined values for noncommuting observables. Such state-dependent formulations, especially entropic formulations [1, 16, 2], have been of tremendous use in quantum information theory so far, in particular in ensuring the security of quantum key distribution [15, 5]. For a short history of joint measurability and the error disturbance tradeoff and further references, see the full version of this submission [12].

In this submission we take a directly operational approach to the original versions of the uncertainty principle, by quantifying error and disturbance in terms of the probability that the actual behavior of the apparatus can be distinguished from a relevant hypothetical behavior, in any experiment whatsoever. This results in state-independent measures which are conceptually simple and unambiguous. We find new uncertainty relations for both joint measurability and the error-disturbance tradeoff of two arbitrary observables of discrete quantum systems. Our relations constrain the characteristics of possible measurement devices themselves, as opposed to entire experimental setups, which include the properties of the input state. Thus they are useful in constraining the behavior of channels as opposed to the properties of states. For instance, we use our relations to show that if a quantum channel faithfully transmits elements of a orthonormal basis, then the complementary channel can only poorly transmit the conjugate basis. Directly operational versions of this notion have only been previously formalized for special cases. It can be used, for example, to construct leakage-resilient classical computers from fault-tolerant quantum computers [9].

Background. All uncertainty relations ultimately spring from the same source, the requirement that the measurement process itself be treated as dynamical process according to the laws

of quantum mechanics. The relations presented here are both relatively simple consequences of a basic structure theorem on quantum dynamics, the continuity of the Stinespring representation [8, 7]. We hence assume in the following that the measurement device is described by a quantum channel, with mapping states in the input state space, $\mathsf{S}(\mathcal{H}_A)$, to states in the output state space, $\mathsf{S}(\mathcal{H}_B)$, conditioned on the classical outcome of the measurement. As mentioned before, we are interested in the probability $p_{\text{dist}}(\mathcal{E}, \mathcal{E}')$ that one can distinguish the operation of one apparatus $\mathcal{E}$ from another $\mathcal{E}'$ in any test whatsoever, when the two are chosen with equal *a priori* probability. Since this probability ranges from $\frac{1}{2}$ (we can always just make a random guess) to 1, it is more convenient to consider the distinguishability measure $\delta(\mathcal{E}, \mathcal{E}') := 2p_{\text{dist}}(\mathcal{E}, \mathcal{E}') - 1$. Fortunately, this quantity is exactly equal to one half of the diamond norm difference between the two channels. Note that we hence also allow for tests using inputs entangled with an additional system; that this improves distinguishability is discussed in the full version of this submission [12].

Joint measurability. Joint measurability of two observables X and Z is naturally concerned with how well a single apparatus $\mathcal{A}_{X,Z}$ can simultaneously approximate both *ideal measurements*, call them $\mathcal{Q}_X$ and $\mathcal{Q}_Z$. Any such device has of course two classical outputs, one for each observable, which we denote by R_X and R_Z. The actual measurement $\mathcal{M}_X$ of X only takes the R_X outcome into account, and similarly for $\mathcal{M}_Z$. Then, we are specifically interested in the two types of *error* inherent to the apparatus, namely how well the marginals of the apparatus compare to the ideal measurements, quantified by $\varepsilon_X(\mathcal{A}_{X,Z}) := \delta(\mathcal{M}_X, \mathcal{Q}_X)$ and $\varepsilon_Z(\mathcal{A}_{X,Z}) := \delta(\mathcal{M}_Z, \mathcal{Q}_Z)$.

We expect that, for incompatible or complementary observables, these quantities cannot both be small. We may quantify the complementarity of X and Z in terms of their eigenstates $|\varphi_x\rangle$ and $|\vartheta_z\rangle$, as follows. Letting $r(X;Z) := \frac{1}{\sqrt{2}}\left(1 - \min_x \max_z |\langle\varphi_x|\vartheta_z\rangle|^2\right)$, the measure of complementarity is $c_1(X,Z) := \max\{r(X;Z), r(Z;X)\}$. Then we have the following uncertainty relation.

Theorem 1 (Joint Measurability)**.** *For any apparatus $\mathcal{A}_{X,Z}$ which attempts to jointly measure two finite-dimensional observables X and Z,*

$$\varepsilon_X(\mathcal{A}_{X,Z})^{\frac{1}{2}} + \varepsilon_Z(\mathcal{A}_{X,Z})^{\frac{1}{2}} \geq c_1(X,Z). \tag{1}$$

The full proof can be found in [12], but let us mention that the main idea is to model the approximate joint measurement as a quantum channel, and then use the aforementioned structure theorem on quantum dynamics, the continuity of the Stinespring representation: Since $\mathcal{M}_X$ and $\mathcal{M}_Z$ are defined from the same apparatus, they share a Stinespring isometry, say V. This isometry is close to appropriate isometries W_X and W_Z for $\mathcal{Q}_X$ and $\mathcal{Q}_Z$ as measured by ε_X and ε_Z, respectively. By the triangle inequality for the isometry distance, we now have a relation for the distance between W_X and W_Z, which can be evaluated by making use of properties of the ideal measurements.

Error disturbance tradeoff. Next we turn to the tradeoff between the approximation error of a given apparatus $\mathcal{A}_X$ for measuring observable X and the disturbance caused to the observable Z. Again $\mathcal{A}_X$ produces the classical result in R_X, and the approximation error $\varepsilon_X(\mathcal{A}_X)$ is precisely the same as defined in the previous section. Now we are also interested in the quantum system S' containing the post-measurement state produced by the action of $\mathcal{A}_X$, and in particular the action of the observable Z. Complete disturbance to Z amounts to its eigenstates all being mapped to a fixed output. In the worst case, this holds even when conditioning on the classical outcome of the $\mathcal{A}_X$ apparatus. That is, it is not possible to perform some subsequent "recovery" operation conditional on the measurement outcome which restores the Z observable; this stronger notion of disturbance was recently used by Buscemi et al. [3]. Our measure of disturbance is how well the action of $\mathcal{A}_X$ approximates a channel with a constant output on both R_X and S' when both channels are input with eigenstates of Z (or mixtures thereof). To ensure that all inputs to $\mathcal{A}_X$ are mixtures of Z eigenstates, we may first perform the ideal non-selective measurement $\mathcal{Q}_Z^\natural$, which measures the the state in the Z basis and discards the result. Then

the post-measurement state is necessarily diagonal in the Z basis. Therefore, the disturbance is large if the map $\mathcal{A}_X \circ \mathcal{Q}_Z^\natural$ is close to a map $\mathcal{C}$ which has constant output for any input state ϱ. We are thus led to a disturbance measure of the form $\eta_Z(\mathcal{A}_X) := \frac{d-1}{d} - \min_{\mathcal{C}} \delta(\mathcal{A}_X \circ \mathcal{Q}_Z^\natural, \mathcal{C})$, since a better approximation means greater disturbance. We note that the quantity is always positive [12]. As with joint measurement, we expect that both $\varepsilon_X(\mathcal{A}_X)$ and $\eta_Z(\mathcal{A}_X)$ cannot both be small if X and Z are incompatible. We again measure complementarity in terms of the eigenvectors, but this time by the function $c_2(X;Z) := \frac{d-1}{d} - \max_z \sum_x \{\frac{1}{d} - |\langle \varphi_x | \vartheta_z \rangle|^2\}_+$, where $\{x\}_+ = \max\{x, 0\}$ and $d = \dim(\mathcal{H}_S)$. Then we have the following uncertainty relation, whose proof is again based on the continuity of the Stinespring representation and can be found in the full version.

Theorem 2 (Error-Disturbance Tradeoff)**.** *For observables X and Z, any apparatus $\mathcal{A}_X$ which attempts to gain information about observable X satisfies*

$$\sqrt{2}\, \varepsilon_X(\mathcal{A}_X)^{\frac{1}{2}} + \eta_Z(\mathcal{A}_X) \geq c_2(X;Z). \tag{2}$$

Applications in Quantum Information Processing. The action of every quantum channel $\mathcal{N}$ can be described by letting the input system interact with some environment, and then disregarding the state on this additional system. If we instead disregard the original output system, the corresponding quantum channel is called the *complement* $\mathcal{N}^\sharp$ of $\mathcal{N}$.

A useful tool in the construction of quantum information processing protocols is the link between reliable transmission of X eigenstates through a channel $\mathcal{N}$ and Z eigenstates through $\mathcal{N}^\sharp$, particularly when the observables X and Z are maximally complementary, i.e. $|\langle \varphi_x | \vartheta_z \rangle|^2 = \frac{1}{d}$ for all x, z. Due to the uncertainty principle, we expect that a channel cannot reliably transmit the bases to both the environment and the actual output system, since this would provide a means to simultaneously measure X and Z. This link has been used by Shor and Preskill to prove the security of quantum key distribution [14] and by Devetak to determine the quantum channel capacity [4]. Entropic state-preparation uncertainty relations from [1, 16] can be used to understand both results, as shown in [10, 11]. However, the above approach has the serious drawback that it can only be used in cases where the specific X-basis transmission over $\mathcal{N}$ and Z-basis transmission over $\mathcal{N}^\sharp$ are in some sense compatible and not *counterfactual*; because the argument relies on a state-dependent uncertainty principle, both scenarios must be compatible with the same quantum state. Using Theorem 2 we can extend the method above to counterfactual uses of arbitrary channels $\mathcal{N}$. If acting with the channel $\mathcal{N}$ does not substantially affect the possibility of performing an X measurement, then Z-basis inputs to $\mathcal{N}^\sharp$ yield an essentially constant output.

Corollary 1. *Given a channel $\mathcal{N}$ and complementary channel $\mathcal{N}^\sharp$, suppose that there exists a measurement Λ_X such that $\delta(\mathcal{Q}_X, \Lambda_X \circ \mathcal{N}) \leq \varepsilon$. Then there exists a constant channel $\mathcal{C}$ such that $\delta(\mathcal{N}^\sharp \circ \mathcal{Q}_Z^\natural, \mathcal{C}) \leq 2\sqrt{\varepsilon} + \frac{d-1}{d} - c_2(X;Z)$. For maximally complementary X and Z, $\delta(\mathcal{N}^\sharp \circ \mathcal{Q}_Z^\natural, \mathcal{C}) \leq 2\sqrt{\varepsilon}$.*

This formulation is important because in more general cryptographic scenarios we are interested in the worst-case behavior of the protocol, not the average case under some particular probability distribution. For instance, in [9] the goal is to construct a classical computer resilient to leakage of Z-basis information by establishing that reliable X basis measurement is possible despite the interference of the eavesdropper. However, such an X measurement is entirely counterfactual and cannot be reconciled with the actual Z-basis usage, as the Z-basis states will be chosen *deterministically* in the classical computer. An additional benefit of Corollary 1 in this scenario is that we may allow the classical computer to be noisy, i.e. undergo errors which flip the Z basis states. Leakage-resilience is neverthess ensured if reliable X basis measurement is still possible.

Motivated by these considerations, we expect that our relations and its implications will turn out to be useful for the study of problems within Quantum Information Theory, as it is the case for entropic formulations of the uncertainty principle.

References

[1] Mario Berta, Matthias Christandl, Roger Colbeck, Joseph M. Renes, and Renato Renner. The uncertainty principle in the presence of quantum memory. *Nature Physics*, 6:659–662, July 2010.

[2] Mario Berta, Matthias Christandl, Fabian Furrer, Volkher B. Scholz, and Marco Tomamichel. Continuous variable entropic uncertainty relations in the presence of quantum memory. arXiv e-print 1308.4527, August 2013.

[3] Francesco Buscemi, Michael J.W. Hall, Masanao Ozawa, and Mark M. Wilde. Noise and disturbance in quantum measurements: An information-theoretic approach. *Physical Review Letters*, 112(5):050401, February 2014.

[4] Igor Devetak. The private classical capacity and quantum capacity of a quantum channel. *IEEE Transactions on Information Theory*, 51(1):44– 55, 2005.

[5] F. Furrer, T. Franz, M. Berta, A. Leverrier, V. B. Scholz, M. Tomamichel, and R. F. Werner. Continuous variable quantum key distribution: Finite-key analysis of composable security against coherent attacks. *Physical Review Letters*, 109(10):100502, September 2012.

[6] W. Heisenberg. Über den anschaulichen inhalt der quantentheoretischen kinematik und mechanik. *Zeitschrift für Physik*, 43(3):172–198, March 1927.

[7] D. Kretschmann, D. Schlingemann, and R.F. Werner. The information-disturbance tradeoff and the continuity of stinespring's representation. *IEEE Transactions on Information Theory*, 54(4):1708–1717, 2008.

[8] Dennis Kretschmann, Dirk Schlingemann, and Reinhard F. Werner. A continuity theorem for stinespring's dilation. *Journal of Functional Analysis*, 255(8):1889–1904, October 2008.

[9] Felipe G. Lacerda, Joseph M. Renes, and Renato Renner. Classical leakage resilience from fault-tolerant quantum computation. *arXiv:1404.7516 [quant-ph]*, April 2014.

[10] Joseph M. Renes. Duality of privacy amplification against quantum adversaries and data compression with quantum side information. *Proceedings of the Royal Society A*, 467(2130):1604–1623, June 2011.

[11] Joseph M. Renes. The physics of quantum information: Complementarity, uncertainty, and entanglement. *International Journal of Quantum Information*, 11(08):1330002, January 2014.

[12] Joseph M Renes and Volkher B Scholz. Operationally-motivated uncertainty relations for joint measurability and the error-disturbance tradeoff. *arXiv:1402.6711 [quant-ph]*, 2014.

[13] H. P. Robertson. The uncertainty principle. *Physical Review*, 34(1):163, July 1929.

[14] Peter W. Shor and John Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Physical Review Letters*, 85(2):441, July 2000.

[15] Marco Tomamichel, Charles Ci Wen Lim, Nicolas Gisin, and Renato Renner. Tight finite-key analysis for quantum cryptography. *Nature Communications*, 3:634, January 2012.

[16] Marco Tomamichel and Renato Renner. Uncertainty relation for smooth entropies. *Physical Review Letters*, 106(11):110506, March 2011.

Institute for Theoretical Physics, ETH Zurich, Wolfgang-Pauli-Str. 27, 8093 Zurich, Switzerland