Quantifying incompatibility beyond entropic uncertainty

Srijita Kundu[1] and Prabha Mandayam[2]
[1]*Chennai Mathematical Institute, Siruseri, Chennai - 603103, India*
[2]*Department of Physics, Indian Institute of Technology Madras, Chennai - 600036, India*
(Dated: September 12, 2014)

Characterizing the mutual incompatibility of a set of quantum observables is an important question both from a quantum cryptographic as well as a foundational point of view. While Heisenberg's uncertainty principle [1, 2] was the first quantitative statement on incompatibility of a pair of canonically conjugate observables, later formulations in terms of entropic quantities characterize the incompatibility of any set of observables via entropic uncertainty relations (EURs) (see [3] for a recent review). EURs play an important role in the security of quantum cryptographic tasks [4–6], and are often thought to provide a measure of incompatibility. However, EURs give rise to a trivial bound whenever the observables in question share a single common eigenvector. This suggests that EURs cannot be thought of as *measures* of incompatibility in general, and, that there is a need to look beyond the standard entropic uncertainty formalism.

Recently, alternate measures have been proposed [7, 8] which aim to go beyond the standard EUR formalism in quantifying incompatibility. Formally, and operationally, these measures depart significantly from other approaches that aim to extend the scope of standard entropic uncertainty framework [9–11]. In this work, we focus on the operational measure ($\mathcal{Q}$) defined in [7], which captures the incompatibility of a set of non-commuting observables as manifest in the non-orthogonality of their eigenstates. It was shown [7] that the measure $\mathcal{Q}$ satisfies all the desired properties: it is zero when the observables commute, strictly greater than zero when they do not, and is maximum when they are mutually unbiased.

In this work, we seek to clarify the exact relation between this operational approach to quantifying incompatibility and the standard EUR formalism. We evaluate $\mathcal{Q}$ for a pair of observables that commute on a subspace, thus providing an explicit example of a class of observables for which the measure $\mathcal{Q}$ goes beyond EURs in quantifying incompatibility. For a general set of observables we prove that the measure $\mathcal{Q}$ is greater than or equal to the lower bound on a corresponding EUR.

Furthermore, we make precise the role played by the measure $\mathcal{Q}$ in QKD – for a QKD protocol whose signal ensemble comprises the eigenstates of a set of quantum observables, we show that the measure $\mathcal{Q}$ is in fact the minimum error rate caused by an eavesdropper adopting an intercept-resend strategy. Finally, we evaluate $\mathcal{Q}$ for a pair of qubit observables, and obtain a lower bound for the incompatibility of *any* set of observables, which is efficiently computable via a semidefinite program (SDP).

We briefly summarize our results here and refer to the technical attachment for further details and proofs.

An operational measure of incompatibility: Consider a set of N non-degenerate, noncommuting observables $\{A^{(1)}, A^{(2)}, \ldots, A^{(N)}\}$ in a d-dimensional Hilbert space $\mathcal{H}_d$. Since such a set of noncommuting observables does not admit a complete set of common eigenstates, atleast some of their eigenstates must be nonorthogonal. Let $|\psi_j^{(i)}\rangle\langle\psi_j^{(i)}|$ denote the j^{th} eigenstate of the i^{th} observable $A^{(i)}$. Then, the mutual incompatibility of the observables $\{A^{(i)}\}$ implies that the states in the ensemble $\mathcal{S} \equiv \{|\psi_j^{(i)}\rangle\langle\psi_j^{(i)}|\}$, $i \in [N]$, $j \in [d]$ are not perfectly distinguishable. The more incompatible the observables $\{A^{(i)}\}$ are, the lesser is the fidelity with which their eigenstates can be distinguished. The incompatibility $\mathcal{Q}(A^{(1)}, A^{(2)}, \ldots, A^{(N)})$ can therefore be defined as the *complement* of the best possible fidelity obtained in a quantum state estimation process for the ensemble of their eigenstates.

The maximum fidelity that can obtained in a state estimation process for states drawn from the ensemble $\mathcal{S}$ with equal probability ($\frac{1}{Nd}$) is,

$$F_{\mathcal{S}}^{\max} = \frac{1}{Nd} \sup_{\mathcal{M},\mathcal{R}} \sum_{a,i,j} \langle \psi_j^{(i)} | M_a | \psi_j^{(i)} \rangle \langle \psi_j^{(i)} | \sigma_a | \psi_j^{(i)} \rangle, \tag{1}$$

where the maximization is over all positive operator valued measures (POVMs) $\mathcal{M}$ with elements $\{M_a\}$ ($0 \leq M_a \leq \mathbb{I}$, $\sum_a M_a = \mathbb{I}$), and state reconstruction maps $\mathcal{R} : a \to \sigma_a$, such that, when the measurement outcome is a, the state σ_a is prepared. The mutual incompatibility $\mathcal{Q}$ of the observables $\{A^{(1)}, \ldots, A^{(N)}\}$ is then defined as [7],

$$\mathcal{Q}(A^{(1)}, \ldots, A^{(N)}) = 1 - F_{\mathcal{S}}^{\max}. \tag{2}$$

Since $\mathcal{Q}(A^{(1)}, \ldots, A^{(N)}) = 0$ if and only if the observables $\{A^{(1)}, \ldots, A^{(N)}\}$ all commute. The measure $\mathcal{Q}$ thus captures the incompatibility of *any* set of observables.

Relevance in quantum cryptography : The measure $\mathcal{Q}$ is of direct relevance in the context of quantum key distribution (QKD) protocols of the *prepare and measure* type [12]. Consider a QKD protocol in which Alice transmits pure states $|\psi_j^{(i)}\rangle\langle\psi_j^{(i)}|$ drawn uniformly at random from the ensemble $\mathcal{S}$. The eavesdropper employs an "intercept-resend strategy" which consists of a measurement $\mathcal{M}$ described by a POVM with elements $\{M_a\}$, followed by a state reconstruction map $\mathcal{R} : a \to \sigma_a$, such that, when the measurement outcome is a, the intercepted state is replaced with the state σ_a and sent to Bob.

It is known [7] that the measure $\mathcal{Q}(A^{(1)}, \ldots, A^{(N)})$ is simply the complement of the *accessible fidelity*, which is the best possible fidelity an eavesdropper employing an intercept-resend strategy can obtain in such a QKD protocol [13]. Here, we show a more direct, quantitative relation between the incompatibility of a set of observables and the error rate caused by the presence of an eavesdropper in a corresponding QKD protocol.

Lemma 1. *For a QKD protocol whose signal states are drawn uniformly at random from the eigenstate ensemble $\mathcal{S}$, the measure $\mathcal{Q}(A^{(1)}, \ldots, A^{(N)})$ is the attainable lower bound on the error rate caused by an eavesdropper adopting an intercept-resend strategy.*

Incompatibility and entropic uncertainty: For a set of N observables $\{A^{(1)}, A^{(2)}, \ldots, A^{(N)}\}$, an entropic uncertainty relation (EUR) seeks to lower bound the average of the entropies associated with a measurement of each observable $A^{(i)}$ on distinct yet identically prepared copies of a state $|\phi\rangle \in \mathcal{H}_d$), as follows:

$$\inf_{|\phi\rangle} \frac{1}{N} \sum_{i=1}^{N} H_\alpha(A^{(i)}, |\phi\rangle) \geq c_\alpha(A^{(1)}, \ldots, A^{(N)}),$$

where $H_\alpha(.)$ denotes the entropy function of choice. Here, we present an example of a class of observables for which $\mathcal{Q}$ is strictly a better measure of incompatibility, namely, observables that commute on a subspace. Such observables are often encountered in quantum theory, for example, in the theory of angular momentum, where the operators L_x and L_z do not commute but still have the $l = 0$ state as a common eigenvector.

Consider a pair of non-degenerate observables A, B that commute over a subspace of dimension d_c and are mutually unbiased [19] in the $(d - d_c)$-dimensional subspace where they do not commute. We show that the mutual incompatibility of such a pair of observables is given by,

$$\mathcal{Q}(A, B) = \frac{1}{2}\left(1 - \frac{d_c + 1}{d}\right). \tag{3}$$

Since EURs attain a trivial (zero) lower bound for such a pair of observables, this example clearly establishes that the measure $\mathcal{Q}$ goes beyond EURs in quantifying the incompatibility of a general sets of quantum observables. More generally, for *any* set of observables, we show that the measure $\mathcal{Q}$ and an EUR lower bound are related as follows.

Theorem 2. *For a set of N non-degenerate observables $\{A^{(1)}, A^{(2)}, \ldots, A^{(N)}\}$ with an associated ensemble of eigenstates $\mathcal{S}$, the incompatibility $\mathcal{Q}(A^{(1)}, A^{(2)}, \ldots, A^{(N)})$ is bounded from below by the average Tsallis T_2 entropy [14][20], that is,*

$$\mathcal{Q}(A^{(1)}, A^{(2)}, \ldots, A^{(N)}) \geq \min_{|\phi\rangle} \frac{1}{N} \sum_i T_2(A^{(i)}; |\phi\rangle). \tag{4}$$

Equality holds iff the POVM $\mathcal{M} \equiv \{M_a\}$ achieving the optimal fidelity of the ensemble $\mathcal{S}$ is **symmetric**, *that is, the individual the POVM elements M_a all achieve the same average fidelity for the ensemble $\mathcal{S}$.*

Incompatibility of qubit observables: For a pair of observables A, B acting on $\mathcal{H}_2$, and parameterized by real vectors $\vec{a}, \vec{b} \in \mathbb{R}^3$ respectively, we obtain an exact expression for their mutual incompatibility:

$$\mathcal{Q}(A, B) = \frac{1}{4} \left(1 - |\cos \delta|\right), \tag{5}$$

where, $\vec{a} \cdot \vec{b} = \cos \delta$. Comparing with the known lower bound on T_2 entropy [15] for a pair of qubit observables, we see that the condition for equality in Theorem 2 is met, and that the inequality (4) is indeed saturated in this case.

An efficiently computable lower bound for $\mathcal{Q}$: It is not known if the incompatibility $\mathcal{Q}$ of a general set of observables is efficiently computable. In fact, evaluating the maximum fidelity $F_{\mathcal{S}}^{\max}$ attainable in a quantum state estimation process for a general ensemble of states $\mathcal{S}$ has been shown to involve a sequence of semi-definite programs (SDPs) [16]. Here, we show that for any set of observables, the measure $\mathcal{Q}$ has an efficiently computable lower bound, by recasting the maximum fidelity function as a matrix norm [17]. Specifically,

$$\mathcal{Q}(A^{(1)}, \ldots, A^{(N)}) \geq 1 - \min_{\substack{\rho : \rho \succ 0 \\ \mathrm{Tr}(\rho)=1}} ||\mathcal{A}_\rho||_\infty, \tag{6}$$

where $||.||_\infty$ is the operator norm defined as $||M||_\infty = \sup_{\|\alpha\|=1} \langle \alpha | M | \alpha \rangle$, and the operator $\mathcal{A}_\rho$ is,

$$\mathcal{A}_\rho = \sum_{i,j} |\psi_j^i\rangle\langle\psi_j^i| \otimes \left(\rho^{-1/2} |\psi_j^i\rangle\langle\psi_j^i| \rho^{-1/2}\right).$$

The lower bound in Eq. (6) involves minimizing the maximum eigenvalue of a positive operator, subject to positive semidefinite constraints, and can be efficiently computed via a semidefinite program [18].

In summary, we establish a quantitative relation between two seemingly different approaches to quantifying incompatibility, namely, the operational measure $\mathcal{Q}$ originally proposed in [7] and entropic uncertainty. We show that evaluating $\mathcal{Q}$ for a set of observables $\{A^{(1)}, \ldots, A^{(N)}\}$ is of direct relevance in analyzing QKD protocols involving the associated ensemble $\mathcal{S}$ of eigenstates, since $\mathcal{Q}$ is the attainable lower bound on the error rate caused by an eavesdropper adopting an intercept-resend strategy. We also address the problem of evaluating the incompatibility of a general set of observables by providing an efficiently computable lower bound on the measure $\mathcal{Q}$.

---

[1] W. Heisenberg, Zeitschrift für Physik **43**, 172 (1927).

[2] H. Robertson, Physical Review **34**, 163 (1929).
[3] S. Wehner and A. Winter, New Journal of Physics **12**, 025009 (2010).
[4] M. Koashi (2005), quant-ph/0505108.
[5] J. M. Renes and J.-C. Boileau, Physical Review A **78**, 032335 (2008).
[6] S. Wehner, C. Schaffner, and B. M. Terhal, Physical Review Letters **100**, 220502 (2008).
[7] S. Bandyopadhyay and P. Mandayam, Physical Review A **87**, 042120 (2013).
[8] P. Mandayam and M. D. Srinivas, PRA **89**, 062112 (2014).
[9] J. Oppenheim and S. Wehner, Science **330**, 1072 (2010).
[10] S. Friedland, V. Gheorghiu, and G. Gour, Physical review letters **111**, 230401 (2013).
[11] M. Tomamichel and E. Hänggi, Journal of Physics A: Mathematical and Theoretical **46**, 055301 (2013).
[12] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Reviews of modern physics **81**, 1301 (2009).
[13] C. A. Fuchs and M. Sasaki, Quantum Information and Computation **3**, 377 (2003).
[14] C. Tsallis, J. Stat. Phys. **51**, 479 (1988).
[15] P. Mandayam and M. D. Srinivas, arXiv preprint arXiv:1402.7311 (2014).
[16] M. Navascués, Physical Review Letters **100**, 070503 (2008).
[17] G. Chiribella and J. Xie, Phys. Rev. Lett. **110**, 213602 (2013).
[18] S. Boyd and L. Vandenberghe, *Convex Optimization* (Cambridge University Press, 2004).
[19] A pair of orthonormal bases $\{|a_i\rangle\}$, $\{|b_i\rangle\}$ in $\mathcal{H}_d$ is said to be mutually unbiased iff $|\langle a_i|b_j\rangle = \frac{1}{d}$, for all i, j.
[20] If $\{p^{A^{(i)}}_{|\phi\rangle}(j)\}$ denote the probability distribution over the outcomes of a measurement of $A^{(i)}$ on state $|\phi\rangle$, the Tsallis entropy T_2 of this distribution is defined as, $T_2(A^{(i)};|\phi\rangle) = 1 - \sum_j (\, p^{A^{(i)}}_{|\phi\rangle}(j)\,)^2$