An Operational Measure of Incompatibility of Noncommuting Observables

Somshubhro Bandyopadhyay[1] and Prabha Mandayam[2]

[1]*Department of Physics and Center for Astroparticle Physics and Space Science, Bose Institute, Block EN, Sector V, Bidhan Nagar, Kolkata 700091, India*

[2]*The Institute of Mathematical Sciences, C. I. T. Campus, Taramani, Chennai 600113, India*

Uncertainty relations are often considered to be a measure of incompatibility of noncommuting observables. However, such a consideration is not valid in general, motivating the need for an alternate measure that applies to any set of noncommuting observables. We present an operational approach to quantifying incompatibility without invoking uncertainty relations. Our measure aims to capture the incompatibility of noncommuting observables as manifest in the nonorthogonality of their eigenstates. We prove that this measure has 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. We also obtain tight upper bounds on this measure for any N noncommuting observables and compute it exactly when the observables are mutually unbiased.

In quantum theory, any observable or a set of commuting observables can in principle be measured with any desired precision. This is because commuting observables have a complete set of simultaneous eigenkets, and therefore, measurement of one does not disturb the measurement result obtained for the other. This no longer holds when the observables do not commute. Noncommuting observables do not have a complete set of common eigenkets, and therefore it is impossible to specify definite values simultaneously. This is the essence of the celebrated uncertainty principle [1, 2]. Uncertainty relations [1–15, 19] express the uncertainty principle in a quantitative way by providing a lower bound on the "uncertainty" in the result of a simultaneous measurement of noncommuting observables.

Observables are defined to be compatible when they commute, and incompatible when they do not. The uncertainty principle, therefore, is a manifestation of the incompatibility of noncommuting observables. Despite the conceptual importance of incompatible observables and applications of such observables in quantum state determination [32–34] and quantum cryptography [24, 25, 27–29], there does not seem to be a good general measure of their incompatibility, although entropic uncertainty relations (EURs) have often been considered for this purpose (see, for example, [14, 16–18]).

Consider, for example, the EUR due to Maassen and Uffink [4]. For any quantum state $\rho \in \mathscr{H}$ with $\dim \mathscr{H} = d$, and measurement of any two observables A and B with eigenvectors $\{|a_i\rangle\}$ and $\{|b_i\rangle\}$, respectively, it was shown that [4]

$$\frac{1}{2}\left(H\left(A|\rho\right)+H\left(B|\rho\right)\right) \;\geq\; -\log c, \tag{1}$$

where $c = \max|\langle a|b\rangle|\colon |a\rangle \in \{|a_i\rangle\}, |b\rangle \in \{|b_i\rangle\}$, and $H\left(X|\rho\right) = -\sum_{i=1}^{d}\langle x_i|\rho|x_i\rangle \log\langle x_i|\rho|x_i\rangle$ for $X \in \{A,B\}$ is the Shannon entropy (all logarithms are taken to base 2). Observe that the RHS of the above inequality is independent of ρ. The incompatibility of the observables A and B can be measured by either the sum of the entropies [LHS of (1)] minimized over all ρ (if it is not known whether equality is achieved) or the lower bound when equality is achieved for some state. We then say that a set of observables is more incompatible than another if the sum (or the lower bound) takes on a larger value. It is clear from the above inequality that a pair of observables is most incompatible when the observables are mutually unbiased. Incompatibility of more than two observables can be similarly quantified via a generalized form of the inequality (1) [14] when such an inequality can be found.

However, it is easy to see why inequality (1) is not a satisfactory measure of incompatibility for *all* pairs of incompatible observables. This is because both sides of the inequality could be zero even when the observables do not commute. This happens, for example, when the noncommuting observables A and B are such that they commute on a subspace. Such observables have one or more common eigenvectors but not all eigenvectors are common because the observables do not commute. For such a pair of observables both sides of inequality (1) are identically zero even though the observables are known to be incompatible. Thus, uncertainty relations can only quantify incompatibility when the observables do not have any common eigenvector. This shows that uncertainty relations cannot be considered as a valid measure of incompatibility for *all* sets of noncommuting observables, thus motivating the present work. Furthermore, incompatibility of more than two observables is much less understood because uncertainty relations (in cases where they are indeed a good measure) are known only for some special classes of observables [10–12, 15, 19]. Even for these cases maximally tight uncertainty relations are not always known to exist [13, 14].

Here, we present an operational approach to quantifying the incompatibility of any set of N noncommuting observables. Since noncommuting observables do not have a complete set of common eigenkets, some of the eigenstates, if not all, corresponding to different noncommuting observables must be nonorthogonal. We therefore suggest a measure that quantifies incompatibility of the observables as manifest in the nonorthogonality of their eigenstates. We show that our measure applies to any set of noncommuting observables (even if the observables commute on a subspace) and has the following desirable properties. It is zero when the observables commute, strictly greater than zero when they do not (note that the approach based on an uncertainty relation fails in this regard), and maximum when they are mutually unbiased. We also obtain nontrivial upper bounds for any N noncommuting observables, and show that they are tight when $N \leq d+1$. We prove the latter by computing the measure exactly for any N mutually unbiased observables.

Operational Setting: In order to define our measure of incompatibility, we adopt the following operational approach, best understood in the setting of quantum cryptography. We imagine a quantum key distribution (QKD) protocol between Alice and Bob, in presence of an eavesdropper employing an intercept-resend attack. Alice transmits quantum states drawn randomly from an ensemble (signal ensemble) S of equiprobable pure states, where the pure states are taken to be the eigenstates of the noncommuting observables whose incompatibility we wish to quantify. The eavesdropper performs a fixed measurement on every intercepted state (we assume that all transmitted states are intercepted), replaces the original state with some other state based on the measurement outcome, and sends it on to Bob. Our measure is defined as the complement of the accessible fidelity [30, 31] (the best possible average fidelity an eavesdropper can obtain) of the set S. Intuitively, this measure corresponds to the “amount of information” that is *inaccessible* to an eavesdropper.

For any given set $\Pi = \left\{\Pi^1, \Pi^2, ..., \Pi^N\right\}$ of N noncommuting observables acting on a Hilbert space $\mathscr{H}_d$ of dimension d, the signal ensemble is defined as a set of pure states $S(\Pi) = \left\{\Pi^i_j = |\psi^i_j\rangle\langle\psi^i_j|\right\}$, with $i = 1, ..., N$ and $j = 1, ..., d$, where $|\psi^i_j\rangle$ is the j^{th} eigenvector of the observable Π^i. Alice transmits pure states Π^i_j drawn randomly from the set $S(\Pi)$ (probability of each state being equal to $1/Nd$). The eavesdropper employs an intercept-resend strategy comprising of a POVM $\mathbf{M} = \{M_a\}$, and a state reconstruction procedure $\mathbf{A}: a \to \sigma_a$ such that when the measurement outcome is a, the eavesdropper substitutes the intercepted state with the state σ_a and sends this state to Bob. The *average fidelity* of $S(\Pi)$ is then given by:

$$F_{S(\Pi)}(\mathbf{M}, \mathbf{A}) = \frac{1}{Nd} \sum_{ija} \mathrm{Tr}\left(\Pi^i_j M_a\right) \mathrm{Tr}\left(\Pi^i_j \sigma_a\right). \tag{2}$$

The *optimal fidelity* is obtained by maximizing the average fidelity over all measurements and state reconstruction procedures:

$$F_{S(\Pi)} = \sup_{\mathbf{M}} \sup_{\mathbf{A}} \frac{1}{Nd} \sum_{ija} \mathrm{Tr}\left(\Pi^i_j M_a\right) \mathrm{Tr}\left(\Pi^i_j \sigma_a\right). \tag{3}$$

The optimal fidelity represents the best possible average fidelity an eavesdropper can obtain. The measure of incompatibility of the noncommuting observables in the set Π is now defined as

$$Q(\Pi) = 1 - F_{S(\Pi)}. \tag{4}$$

It is clear from the definition that the measure is applicable even when the noncommuting observables $\{\Pi^i\}$ have one or more common eigenvectors. We will say that a set of observables Π_1 is more incompatible than another, say, Π_2, if the former takes on a larger Q value. It is interesting to note that the comparison holds regardless of the number of observables in each set and the dimension of the Hilbert space.

For any set Π of N noncommuting observables, $Q(\Pi)$ can in principle be computed but requires optimization which may be difficult to perform in general. Nevertheless, we obtain a simplified expression of a closely related quantity which might be useful in computing the measure for special classes of observables. In what follows, we formally state the basic properties of Q and give upper bounds on Q which are tight for a set of N mutually unbiased observables. We refer to the arxiv preprint [36] for further details and proofs.

Result 1. *$Q = 0$ for commuting observables and $Q > 0$ when the observables do not commute.*

Result 2 (Upper Bounds)**.** *Any set Π of N noncommuting observables acting on $\mathscr{H}_d$ with $\dim \mathscr{H}_d = d$ satisfies:*

$$Q(\Pi) \leq \left(1-\frac{1}{N}\right)\left(1-\frac{1}{d}\right), \quad N \leq d+1 \tag{5}$$

$$Q(\Pi) \leq \frac{d-1}{d+1}, \quad N \geq d+1 \tag{6}$$

We would like to point out that both upper bounds hold for any N. However, they are competing in the sense that one is better than the other depending on whether $N < d+1$ or $N > d+1$, and are equal when $N = d+1$. Finally, we show that the upper bounds are tight for mutually unbiased observables, namely, observables whose eigenvectors form mutually unbiased bases [32–35]. For N mutually unbiased observables, $\Pi^1, \Pi^2, ..., \Pi^N$, their eigenvectors satisfy:

$$\mathrm{Tr}\left(\Pi^i_j \Pi^i_k\right) = \delta_{jk}; \quad \mathrm{Tr}\left(\Pi^i_j \Pi^k_l\right) = \frac{1}{d} \text{ when } i \neq k. \tag{7}$$

It is known that a complete set of $d+1$ mutually unbiased bases exist in prime and prime powered dimensions [33–35] . For other dimensions, however, the problem remains open.

Result 3 (Exact Expression for Mutually Unbiased Observables:)**.** *Let $\Pi = \{\Pi^1, \Pi^2, ..., \Pi^N\}$ be a set of $N \leq d+1$ mutually unbiased observables acting on $\mathscr{H}_d$ with $\dim \mathscr{H}_d = d$. Then,*

$$Q(\Pi) = \left(1-\frac{1}{N}\right)\left(1-\frac{1}{d}\right) \tag{8}$$

Conclusions: In summary, we have pointed out that uncertainty relations cannot, in general, be considered as a measure of incompatibility of noncommuting observables. This observation leads us to propose a measure of incompatibility that applies to any set of noncommuting observables. The measure relies on two simple facts: When observables do not commute, at least some of their eigenstates must be nonorthogonal, and nonorthogonal quantum states cannot be perfectly distinguished. The measure is shown to satisfy the desired properties, namely, it is zero when the observables commute and strictly greater than zero when they do not. We have also obtained tight upper bounds for any N noncommuting observables and evaluated the measure exactly for mutually unbiased observables.

We note that the underlying physical principle defining our measure and the security of QKD protocols such as BB84 [24] and its generalizations [25–29] is the same. Thus, the exact expression of incompatibility of any N mutually unbiased observables obtained here is expected to help analyze the security of such protocols. Like entropic uncertainty relations, the results presented here might also have potential applications in quantum cryptography [20, 21] and information locking [22]. Furthermore, a recent result [23] shows that entanglement can be detected by local mutually unbiased measurements. It is possible that the results presented here could also help to obtain separability bounds from incompatible measurements, other than mutually unbiased, on the local subsystems.

As a final comment, we feel that alternate measures of incompatibility of observables should be explored for reasons outlined in the Introduction. While this paper suggests only one such measure, the idea behind it is quite general and it is likely that similar quantities might serve as an equally good measure. Of course, it is hard to see how the difficulty of general optimization could be avoided.

[1] W. Heisenberg, Zeitschrift für Physik , 43, 172 (1927).
[2] H. P. Robertson, Physical Review 34, 163 (1929).
[3] D. Deutsch, Physical Review Letters 50, 631 (1983).
[4] H. Maassen, and J. Uffink, Physical Review Letters 60, 1103 (1988).
[5] I. I. Hirschmann, American Journal of Mathematics 79, 152 (1957).
[6] W. Beckner, Annals of Mathematics 102, 159 (1975).
[7] I. Bialynicki-Birula, and J. Mycielski, Communications in Mathematical Physics 44, 129 (1975).
[8] I. Bialynicki-Birula, Physics Letters A 103, 253 (1984).
[9] I. D. Ivanovic, Journal of Physics A: Math. Gen. 25, 363 (1992).
[10] J. Sanchez, Physics Letters A 173, 233 (1993).
[11] J. Sanchez-Ruiz, Physics Letters A 201, 125 (1995).
[12] J. Sanchez-Ruiz, Physics Letters A 244, 189 (1998).
[13] P. Mandayam, S. Wehner, and N. Balachandran, Journal of Mathematical Physics 51, 082201 (2010).
[14] S. Wehner, and A. Winter, New Journal of Physics 12, 025009 (2010).
[15] S. Wehner, and A. Winter, Journal of Mathematical Physics 49, 062105 (2008).
[16] H Maassen, Quantum probability and applications V, Lecture Notes in Mathematics Volume 1442, 1990, pp 263-266 1990 - Springer.
[17] M. A. Ballester, and S. Wehner, Physical Review A 75, 022319 (2007).
[18] A. Azarchs, arXiv preprint quant-ph/0412083, (2004).
[19] P. Hayden, D. Leung, P. Shor, and A. Winter, Communications in Mathematical Physics 250, 371 (2004), IEEE New York.
[20] I. Damgaard, S. fehr, L. Salvail, and C. Schaffner, Proceedings of 46th IEEE FOCS, pp 449-458 (2005),
[21] M. Koashi, New Journal of Physics 11, 045018 (2009).
[22] D. DiVincenzo, M. Horodecki, D. Leung, J. Smolin, and B. Terhal, Physical Review Letters 92, 067902 (2004).
[23] C. Spengler, M. Huber, S. Brierley, T. Adaktylos, B. C. Hiesmayr, Physical Review A 86, 022311 (2012).
[24] C. H. Bennett, and G. Brassard, Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, pp. 175-179 (1984), IEEE New York.
[25] D. Bruss, Physical Review Letters 81, 3018 (1998).
[26] H. Bechmann-Pasquinucci, and N. Gisin, Physical Review A 59, 4238 (1999).
[27] H. Bechmann-Pasquinucci, and W. Tittel, Physical Review A 61, 062308 (2000).
[28] H. Bechmann-Pasquinucci, and A. Peres, Physical Review Letters 85, 3313 (2000).
[29] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Physical Review Letters 88, 127902 (2002).
[30] C. Fuchs, and M. Sasaki, Quantum Information & Computation 3, 377 (2003).
[31] C. Fuchs, Quantum Information & Computation 4, 467 (2004).
[32] T. Durt, B. G. Englert, I. Bengtsson, K. Życzkowski, International Journal of Quantum Information, 8, 535 (2010)
[33] I.D. Ivanovi´c, Journal of Physics A 14, 3241 (1981).
[34] W.K. Wootters and B.D. Fields, Ann. Physics, 191:363–381, 1989.
[35] S. Bandyopadhyay, P.O. Boykin, V. Roychowdhury, and F. Vatan, Algorithmica, 34:512–528, 2002.
[36] S. Bandyopadhyay, and P. Mandayam, arXiv pre-print quant-ph: 1301.4762, URL http://arxiv.org/abs/1301.4762 (2013).