An Operational Measure of Incompatibility of Noncommuting Observables

Somshubhro Bandyopadhyay[1] * 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*

Abstract. 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.

Keywords: QKD, accessible fidelity, mutually unbiased observables

In quantum theory, any observable or a set of commuting observables can in principle be measured with any desired precision. 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]. Uncertainty relations 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 is thus a manifestation of the incompatibility of noncommuting observables. Despite the conceptual importance of quantifying incompatibility and the usefulness of such observables in quantum state discrimination [4] and quantum cryptography [5], there is no good general measure of their incompatibility, although entropic uncertainty relations (EURs) [2] have often been considered for this purpose.

Consider, for example, the EUR due to Maassen and Uffink [3]. For any quantum state $\rho \in \mathcal{H}$ with $\dim \mathcal{H} = d$, and measurement of any two observables A and B with eigenvectors $\{|a_i\rangle\}$ and $\{|b_i\rangle\}$, respectively, it was shown that [3]

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

where $c = \max |\langle a|b\rangle|$: $|a\rangle \in \{|a_i\rangle\}, |b\rangle \in \{|b_i\rangle\}$, and $H\left(X|\rho\right) = -\sum_{i=1}^{d} \langle x_i|\rho|x_i\rangle \log \langle x_i|\rho|x_i\rangle$ is the Shannon entropy. 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 or the lower bound when equality is achieved for some state. A set of observables is said to be more incompatible than another if the sum (or the lower bound) takes on a larger value. It is clear 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), when such an inequality can be found (see [2] for a recent review).

However, (1) is not a satisfactory measure of incompatibility for *all* pairs of incompatible observables, since both sides of the inequality can 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. 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 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 [2].

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 when the observables commute on a subspace.

Operational Setting: To define our measure of incompatibility, we adopt an operational approach, best understood in the setting of quantum cryptography. We imagine a quantum key distribution (QKD) protocol be-

* som@bosemain.boseinst.ac.in

† prabhamd@imsc.res.in

tween Alice and Bob, in presence of an eavesdropper employing an intercept-resend attack. Alice transmits quantum states drawn randomly from an 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. For a set $\Pi = \left\{\Pi^1, \Pi^2, ..., \Pi^N\right\}$ of N noncommuting observables acting on a Hilbert space $\mathcal{H}_d$ of dimension d, the signal ensemble is defined as a set of pure states $S(\Pi) = \left\{\Pi_j^i = |\psi_j^i\rangle\langle\psi_j^i|\right\}$, with $i = 1, ..., N$ and $j = 1, ..., d$, where $|\psi_j^i\rangle$ is the j^{th} eigenvector of the observable Π^i. Alice transmits pure states Π_j^i drawn randomly and equiprobably from the set $S(\Pi)$.

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. Our measure is defined as the complement of the accessible fidelity [6] of the set S. Intuitively, this measure corresponds to the "amount of information" that is *inaccessible* to an eavesdropper.

The *average fidelity* of $S(\Pi)$ is given by:

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

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

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

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

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

It is clear from the definition that the measure is applicable even when the noncommuting observables $\left\{\Pi^i\right\}$ 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.

We show that Q has the following desirable property. 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.

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

We also obtain nontrivial upper bounds for any N noncommuting observables, and show that they are tight when $N \leq d + 1$, by computing the measure exactly for any N mutually unbiased observables, namely, observables whose eigenvectors form mutually unbiased bases [7, 4]. For N mutually unbiased observables, $\Pi^1, \Pi^2, ..., \Pi^N$, their eigenvectors satisfy:

$$\mathrm{Tr}\left(\Pi_j^i \Pi_k^i\right) = \delta_{jk}; \quad \mathrm{Tr}\left(\Pi_j^i \Pi_l^k\right) = \frac{1}{d} \text{ when } i \neq k. \quad (5)$$

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

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

$$Q(\Pi) \leq \frac{d-1}{d+1}, \quad N \geq d + 1 \quad (7)$$

Result 3 *Let $\Pi = \left\{\Pi^1, \Pi^2, ..., \Pi^N\right\}$ be a set of $N \leq d + 1$ mutually unbiased observables acting on $\mathcal{H}_d$ with $\dim \mathcal{H}_d = d$. Then,*

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

We refer to the arxiv pre-print [8] for further details and proofs. In conclusion, we note that the underlying physical principle defining our measure and the security of QKD protocols such as BB84 [5] and its generalizations 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 EURs, the results presented here might also have potential applications in quantum cryptography and entanglement detection [9].

References

[1] W. Heisenberg, Zeitschrift fr Physik , **43**, 172 (1927); H. P. Robertson, Phys Rev **34**, 163 (1929).

[2] S. Wehner, and A. Winter, N J Phys **12**, 025009 (2010).

[3] H. Maassen and J. Uffink, Phys Rev Lett **60**, 1103 (1988);

[4] I.D. Ivanovic, J Phys A **14**, 3241 (1981); W.K. Wootters and B.D. Fields, Ann. Physics, **191**:363–381, (1989).

[5] C. H. Bennett, and G. Brassard, Proc IEEE Conf on Computers, Systems and Signal Processing, Bangalore, India, pp. 175-179 (1984), IEEE New York.

[6] C. Fuchs, and M. Sasaki, Quant Inf & Comp **3**, 377 (2003); C. Fuchs, Quant Inf & Comp **4**, 467 (2004).

[7] S. Bandyopadhyay *et al*, Algorithmica, **34**:512–528, 2002.

[8] S. Bandyopadhyay, and P. Mandayam, arXiv preprint 1301.4762 (2013).

[9] C. Spengler *et al*, Phys Rev A **86**, 022311 (2012).