Joint measurability, steering and entropic uncertainty

H. S. Karthik,‡ A. R. Usha Devi,† and A. K. Rajagopal∗

‡Raman Research Institute, Bangalore 560 080, India
†Department of Physics, Bangalore University, Bangalore-560 056, India
∗Inspire Institute Inc., Alexandria, Virginia, 22303, USA.

Institute of Mathematical Sciences, C.I.T. Campus, Taramani, Chennai, 600113, India
Harish-Chandra Research Institute, Chhatnag Road, Jhunsi, Allahabad 211 019, India.

(Dated: December 3, 2014)

There has been a surge of research activity recently on the role of joint measurability of unsharp observables on non-local features viz., violation of Bell inequality and EPR steering. Here, we investigate the entropic uncertainty relation for a pair of non-commuting observables (of Alice’s system), when an entangled quantum memory of Bob is restricted to record outcomes of jointly measurable POVMs. We show that with this imposed constraint of joint measurability at Bob’s end, the entropic uncertainties associated with Alice’s measurement outcomes – conditioned by the results registered at Bob’s end – obey an entropic steering inequality. Thus, Bob’s non-steerability is intrinsically linked with his inability in predicting the outcomes of Alice’s pair of non-commuting observables with better precision, even when they share an entangled state. As a further consequence, we prove that in the joint measurability regime, the quantum advantage envisaged for the construction of security proofs in quantum key distribution is lost.

PACS numbers: 03.65.Ta, 03.65.Ca

I. INTRODUCTION

In the classical domain physical observables commute with each other and they can all be jointly measured. In contrast, measurements of observables, which do not commute are usually declared to be incompatible in the quantum scenario. However, the notion of compatibility of measurements is captured entirely by commutativity of the observables if one restricts only to sharp projective valued (PV) measurements. In an extended framework, which include measurements of unsharp generalized observables, comprised of positive operator valued measures (POVM), the concept of joint measurability gets delinked from that of commutativity [1–10]. Though non-commuting observables do not admit simultaneous sharp values through their corresponding PV measurements, it is possible to assign unsharp values jointly to compatible positive operator valued (POV) observables. Active research efforts are dedicated [1] 3 5 7 12 15 to explore clear, operationally significant criteria of joint measurability for two or more POVMs and also to identify that incompatible measurements, which cannot be implemented jointly, are necessary to bring out non-classical features. In this context, it has already been recognized [1] 3 5 7 12 14 15 that if one merely confines to local compatible POVMs on parts of an entangled quantum system, it is not possible to witness non-local quantum features like steering (the ability to non-locally alter the states of one part of a composite system by performing measurements on another spatially separated part [16]) and violation of Bell inequality. More specifically, incompatible measurements are instrumental in bringing to surface the violations of various no-go theorems in the quantum world.

In this work, we investigate the entropic uncertainty relation associated with Alice’s measurements of a pair of non-commuting discrete observables with d outcomes, in the presence of Bob’s quantum memory [17] – by restricting to compatible (jointly measurable) POVMs at Bob’s end. We first establish that the sum of entropies of Alice’s measurement results, when conditioned by the outcomes of compatible unsharp POVMs recorded in Bob’s quantum memory, is constrained to obey an entropic steering inequality derived in Ref. [18 19]. This essentially brings out the intrinsic equivalence between the violation of an entropic steering inequality and the possibility of reducing the entropic uncertainty bound of a pair of non-commuting observables with the help of an entangled quantum memory. And as violation of a steering inequality requires [14 15] that (i) the parties share a steerable entangled state and also that (ii) the measurements by one of the parties (Bob) [23] is incompatible, it becomes evident that information stored in Bob’s entangled quantum memory is of no use in reducing the uncertainty of Alice’s pair of non-commuting observables, when Bob can measure only compatible POVMs. Consequently, we prove that the quantum advantage for the construction of security proofs in quantum key distribution (QKD) [17] is lost in the joint measurability regime.

The structure of the paper is organized as follows. In Sec. II we give an overview of generalized POV observables and their joint measurability. Entropic uncertainty relation for Alice’s pair of discrete observables in the presence of Bob’s quantum memory is discussed in Sec. III.

*Electronic address: karthik@rri.res.in
†Electronic address: aruthi@rediffmail.com
‡Electronic address: attipat.rajagopal@gmail.com
It is shown that when Bob is restricted to employ only jointly measurable POVMs, it is not possible to achieve enhanced precision for predicting Alice’s measurement outcomes, even if entangled state is shared between them. Implications of this identification on security proofs in QKD is also outlined. Section IV contains concluding remarks.

II. JOINT MEASURABILITY

We begin by giving an outline of generalized measurement of observables in terms of POVMs. A POVM is a set $\mathcal{E} = \{E(x)\}$ of positive self-adjoint operators $0 \leq E(x) \leq 1$, called effects, satisfying $\sum_x E(x) = \mathbb{1}$; $\mathbb{1}$ denotes the identity operator. When a quantum system is prepared in the state $\rho$, measurement of $\mathcal{E}$ gives an outcome $x$ with probability $p(x) = \text{Tr}[\rho E(x)]$. If $\{E(x)\}$ is a set of complete, orthogonal projectors, then the measurement reduces to the simple case of PV measurement.

Let us consider a collection of POV observables $\mathcal{E}_i = \{E_i(x_i)\}$. They are jointly measurable if there exists a grand POVM $\mathcal{G} = \{G(\lambda); 0 \leq G(\lambda) \leq \mathbb{1}, \sum_\lambda G(\lambda) = \mathbb{1}\}$ from which the observables $\mathcal{E}_i$ can be constructed as follows. A measurement of the generalized observable $\mathcal{G}$ is carried out in a state $\rho$ and the probability of obtaining the outcome $\lambda$ is denoted by $p(\lambda) = \text{Tr}[\rho G(\lambda)]$. If the elements of the POVMs $\mathcal{E}_i = \{E_i(x_i)\}$ can be constructed as marginals of the grand POVM $\mathcal{G} = \{G(\lambda), \lambda = \{x_1, x_2, \ldots \}\}$ i.e., $E_1(x_1) = \sum_{x_2, x_3, \ldots} G(x_1, x_2, x_3, \ldots)$, $E_2(x_2) = \sum_{x_1, x_3, \ldots} G(x_1, x_2, x_3, \ldots)$ and so on, the set $\{\mathcal{E}_i\}$ of POVMs is jointly measurable.

In general, if the effects $E_i(x_i)$ can be constructed in terms of $G(\lambda)$ as $E_i(x_i) = \sum_\lambda p(x_i|i, \lambda) G(\lambda) \quad \forall \ i$, where $0 \leq p(x_i|i, \lambda) \leq 1$ are positive numbers satisfying $\sum_x p(x_i|i, \lambda) = 1$, then the POVMs $\mathcal{E}_i$ are jointly measurable. For all jointly measurable POVMs, the probability $p(x_i|i)$ of the outcome $x_i$ in the measurement of $\mathcal{E}_i$ can be post processed based on the results of measurement of the grand POVM observable $G$: $p(x_i|i) = \text{Tr}[\rho E_i(x_i)] = \sum_\lambda p(\lambda) p(x_i|i, \lambda)$. (2)

More specifically, measurements of compatible POVMs $\mathcal{E}_i$ can be interpreted in terms of a single grand POVM $\mathcal{G}$ (i.e., given the positive numbers $p(x_i|i, \lambda)$, one can construct the probabilities of measuring compatible POVMs $\mathcal{E}_i$ solely based on the results of measurement of $\mathcal{G}$). An important feature that gets highlighted here is that the generalized POV observables are jointly measurable even if they do not commute with each other.

Reconciling to joint measurability within quantum theory results in subsequent manifestation of classical features. In particular, as measurement of a single grand POVM can be used to construct results of measurements of all compatible POVMs, joint measurability entails a joint probability distribution for all compatible observables (though for unsharp values of the observables) in every quantum state. Existence of joint probabilities in turn implies that the set of all Bell inequalities are satisfied, when only compatible measurements are employed. Wolf et. al. have shown that incompatible measurements of a pair of POVMs with dichotomic outcomes are necessary and sufficient for the violation of Clauser-Horne-Shimony-Holt (CHSH) Bell inequality. Further, Quintino et. al. and Vola et. al. have established a more general result that a set of POVMs (with arbitrarily many outcomes) are not jointly measurable if and only if they are useful for non-local quantum steering. It is of interest to explore the limitations imposed by joint measurability on quantum information tasks. In the following, we study the implications of joint measurability on entropic uncertainty relation in the presence of quantum memory.

III. ENTRepT UNCERTAINTY RELATION IN THE PRESENCE OF QUANTUM MEMORY

The Shannon entropies $H(\mathbb{X}) = -\sum_x p(x) \log_2 p(x)$, $H(\mathbb{Z}) = -\sum_z p(z) \log_2 p(z)$, associated with the probabilities $p(x) = \text{Tr}[\rho E_{\mathbb{X}}(x)]$, $p(z) = \text{Tr}[\rho E_{\mathbb{Z}}(z)]$ of measurement outcomes $x$, $z$ of a pair of POV observables $\mathbb{X} \equiv \{E_{\mathbb{X}}(x) | 0 \leq E_{\mathbb{X}} \leq \mathbb{1}; \sum_x E_{\mathbb{X}} = \mathbb{1}\}$, $\mathbb{Z} \equiv \{E_{\mathbb{Z}}(z) | 0 \leq E_{\mathbb{Z}} \leq \mathbb{1}; \sum_z E_{\mathbb{Z}} = \mathbb{1}\}$, quantify the uncertainties of predicting the measurement outcomes in a quantum state $\rho$. Trade-off between the entropies of observables $\mathbb{X}$ and $\mathbb{Z}$ in a finite level quantum system is quantified by the entropic uncertainty relation: $H(\mathbb{X}) + H(\mathbb{Z}) \geq -2 \log_2 C(\mathbb{X}, \mathbb{Z})$, where $C(\mathbb{X}, \mathbb{Z}) = \max_{x,z} \| \sqrt{E_{\mathbb{X}}(x)} \sqrt{E_{\mathbb{Z}}(z)} \|$. (Here, $\|A\| = \text{Tr}[\sqrt{A\,\,A^\dagger}]$).

Consider the following uncertainty game: two players Alice and Bob agree to measure a pair of observables $\mathbb{X}$ and $\mathbb{Z}$. Bob prepares a quantum state of his choice and sends it to Alice. Alice measures $\mathbb{X}$ or $\mathbb{Z}$ randomly and communicates her choice of measurements to Bob. To win the game, Bob’s initial preparation of the quantum state should be such that he is able to predict Alice’s measurement outcomes of the chosen pair of observables $\mathbb{X}$ or $\mathbb{Z}$ with as much precision as possible, when Alice announces which of the pair of observables is measured. In other words, Bob’s task is to minimize the uncertainties in the measurements of a pair of observables $\mathbb{X}$, $\mathbb{Z}$ that were agreed upon initially, with the help of an optimal quantum state. The uncertainties of $\mathbb{X}$, $\mathbb{Z}$ are bounded as in (3), when Bob has only classical information about the state. On the other hand, with the help of a quantum memory (where Bob prepares an entangled state and sends one part of the state to Alice) Bob can beat the uncertainty bound of (3).
共享一个纠缠态与Alice，Bob可以将不确定性界限定为$3$，并可以预测输出的任意一组可观测量$X, Z$的改进精度，通过执行适合的可观测量。Bob的量子存储器在Bob的量子态处于可衡量的情况下，不能达到在不确定性关系中的改善。在其他情况下，已经证明最近$[14,15]$，Bob的测量结果可以导致违反不确定性关系（6）的条件对于可衡量的状态，Bob和Alice可以执行任意一组可观测量，这将导致违反不确定性关系（6）。如果Bob不能远程控制Alice的状态，则Bob的测量结果可以用于确定Bob的量子存储器是否处于可衡量状态。在其他情况下，Bob控制量子存储器的结果可以用于确定Bob的量子存储器是否处于可衡量状态。
to predict Alice’s outcomes by performing unsharp compatible measurements of $X' = \{ E_{X'}(x') \}, x' = \pm 1$ or $Z' = \{ E_{Z'}(z') \}, z' = \pm 1$ on his qubit. The effects $E_{X'}(x'), E_{Z'}(z')$ constituting the binary unsharp qubit observables $X', Z'$ are given by,

$$
E_{X'}(x') = \frac{1}{2} (1 + \eta x' X'),
E_{Z'}(z') = \frac{1}{2} (1 + \eta z' Z'),
$$

where $x', z'$ are the measurement outcomes and $0 \leq \eta \leq 1$ denotes the unsharpness of the fuzzy measurements. Clearly, when $\eta = 1$, the POVM elements $E_{X'}(x'), E_{Z'}(z')$ reduce to their corresponding sharp PV versions (see (7)) $\Pi_{X'}(x'), \Pi_{Z'}(z')$.

$$
H(X|X') + H(Z|Z') = - \sum_{x,x' = \pm 1} p(x,x') \log_2 p(x|x') - \sum_{z,z' = \pm 1} p(z,z') \log_2 p(z|z')
$$

$$
= 2 H[(1 + \eta)/2]
$$

where $H(p) = -p \log_2 p - (1-p) \log_2 (1-p)$ is the binary entropy. As the binary entropy function $H[(1 + \eta)/2] = 0$ only when $\eta = 1$, the trivial lower bound of the uncertainty relation (3) can be reached if Bob too performs sharp PV measurements of the observables $X$ and $Z$ at his end. In other words, Bob can predict the outcomes of Alice’s measurements of $X$ and $Z$ precisely when he employs sharp PV measurements of the same observables. But sharp measurements of $X$ and $Z$ are not compatible. The joint measurability of the unsharp POVMs $X = \{ E_{X'}(x') \}$ and $Z = \{ E_{Z'}(z') \}$ sets the limitation $1/\sqrt{2}$ on the unsharpness parameter.

The joint probabilities $p(x,x')$ (or $p(z,z')$ of Alice’s sharp outcome $x$ (or $z$) and Bob’s unsharp outcome $x'$ (or $z'$), when they both choose to measure the same observable $X$ (or $Z$) at their ends, is obtained to be,

$$
p(x,x') = \langle \psi_{AB} | \Pi_{X}(x) \otimes E_{X'}(x') | \psi_{AB} \rangle = \frac{1}{4} (1 - \eta x x')
$$

$$
p(z,z') = \langle \psi_{AB} | \Pi_{Z}(z) \otimes E_{Z'}(z') | \psi_{AB} \rangle = \frac{1}{4} (1 - \eta z z')
$$

While the right-hand side of the entropic uncertainty relation (3) reduces to zero in this case, the left-hand side can be simplified (see (27)) to obtain,

$$
H(X|X') + H(Z|Z') \geq 1
$$

The joint probabilities $p(x,x')$ (or $p(z,z')$ of Alice’s sharp outcome $x$ (or $z$) and Bob’s unsharp outcome $x'$ (or $z'$), when they both choose to measure the same observable $X$ (or $Z$) at their ends, is obtained to be,

$$
p(x,x') = \langle \psi_{AB} | \Pi_{X}(x) \otimes E_{X'}(x') | \psi_{AB} \rangle = \frac{1}{4} (1 - \eta x x')
$$

$$
p(z,z') = \langle \psi_{AB} | \Pi_{Z}(z) \otimes E_{Z'}(z') | \psi_{AB} \rangle = \frac{1}{4} (1 - \eta z z')
$$

B. Joint measurability and QKD

The entropic uncertainty relation in the presence of quantum memory (1) provides a quantification for the connection between entanglement and uncertainty. Moreover, it has been shown (14) to be useful to derive a lower bound on the secret key rate that can be generated by Alice and Bob in QKD against collective attacks by an adversary Eve. Subsequently more tighter finite-key bound on discrete variable QKD has been derived based on generalized uncertainty relations for smooth min- max- entropies (29). Entropic uncertainty relations have also proved to be of practical use in identifying security proofs of device independent QKD (30). Recently Branciard et. al. (31) showed for the first time that steering and security of one sided device independent (ISDI) QKD are related. In the following, we focus on the implications of joint measurability on the secret key rate in QKD against collective attacks by an adversary Eve.

Suppose that Eve prepares a three party quantum state $\rho_{ABE}$ and gives the $A$, $B$ parts to Alice and Bob, keeping the part $E$ with her. Alice measures the observables $\mathbb{X}$, $\mathbb{Z}$ randomly on the state she receives and Bob tries to predict Alice’s results by his measurements $\mathbb{X}'$, $\mathbb{Z}'$. In order to generate a key, Alice communicates her choice of measurements to Bob. Even if this communication is overheard by Eve, Alice and Bob can generate a secure key – provided the correlations between their measurement outcomes fare better than those between Eve and Alice. More specifically, if the difference between the mutual informations $S(\mathbb{X} : B) = (H_X^E) + S(B) - S(E_{XAB}) = S(E_X^B) - S(\mathbb{X}|B) and
form measurement of compatible POVMs

\[ S(\mathbb{X} : E) = S (\rho_X^E) + S(E) - S (\rho_{AE}^E) = S (\rho_X^E) - S(\mathbb{X}|E) \]

(corresponding to the measurement of \( \mathbb{X} \) at Alice’s end) is positive, Alice and Bob can always generate a secure key.

The amount of key \( K \) that Alice and Bob can generate per state is lower bounded by \[ 32 \]

\[ K \geq S(\mathbb{X} : B) - S(\mathbb{X} : E) = S(\mathbb{X}|E) - S(\mathbb{X}|B) \quad (12) \]

It may be noted that when Alice’s measurement outcomes of \( \mathbb{X} \), \( \mathbb{Z} \) are simultaneously stored in the quantum memories of Eve and Bob respectively, the following trade-off relation for the entropies \( S(\mathbb{X}|E) \), \( S(\mathbb{Z}|B) \) ensures \[ 17 \] \[ 33 \] \[ 54 \]:

\[ S(\mathbb{X}|E) + S(\mathbb{Z}|B) \geq -2 \log_2 C(\mathbb{X}, \mathbb{Z}) \quad (13) \]

And, employing \[ 13 \] in \[ 12 \], one obtains

\[ K \geq S(\mathbb{X}|E) + S(\mathbb{Z}|B) - [S(\mathbb{X}|B) + S(\mathbb{Z}|B)] \geq -2 \log_2 C(\mathbb{X}, \mathbb{Z}) - [S(\mathbb{X}|B) + S(\mathbb{Z}|B)] \quad (14) \]

As \( H(\mathbb{X}|\mathbb{X}') \geq S(\mathbb{X}|B), H(\mathbb{Z}|\mathbb{Z}') \geq S(\mathbb{Z}|B) \), the lower bound of the inequality \[ 14 \] can be simplified to obtain \[ 17 \],

\[ K \geq -2 \log_2 C(\mathbb{X}, \mathbb{Z}) - [H(\mathbb{X}|\mathbb{X}') + H(\mathbb{Z}|\mathbb{Z}')] \quad (15) \]

It is clear that when Bob is constrained to perform measurement of compatible POVMs \( \mathbb{X}', \mathbb{Z}' \), the conditional entropies \( H(\mathbb{X}|\mathbb{X}') \), \( H(\mathbb{Z}|\mathbb{Z}') \) satisfy the entropic steering inequality: \( H(\mathbb{X}|\mathbb{X}') + H(\mathbb{Z}|\mathbb{Z}') \geq -2 \log_2 C(\mathbb{X}, \mathbb{Z}) \) (see \[ 5 \]), in which case the key rate is not ensured to be positive. Bob must be equipped to perform incompatible measurements at his end (so that it is possible to witness violation of the steering inequality by beating the bound \( -2 \log_2 C(\mathbb{X}, \mathbb{Z}) \)) on entropic uncertainties and attain the refined bound of \( -2 \log_2 C(\mathbb{X}, \mathbb{Z}) + S(\mathbb{X}|B) \) as in \[ 5 \] in order that a positive key rate ensues. In other words, quantum advantage for security in QKD against collective attacks by Eve is not envisaged, when Bob is constrained to perform compatible measurements only.

### IV. CONCLUSIONS

Measurement outcomes of a pair of non-commuting observables reveal a trade-off, which is quantified by uncertainty relations. Entropic uncertainty relation \[ 24 \] constrains the sum of entropies associated with the probabilities of outcomes of a pair of observables. An extended entropic uncertainty relation \[ 17 \] brought out that it is possible to beat the lower bound on uncertainties when the system is entangled with a quantum memory. In this paper we have explored the entropic uncertainty relation when the entangled quantum memory is restricted to record the outcomes of jointly measurable POVMs only. With this constraint on the measurements, the entropies satisfy an entropic steering inequality \[ 18 \]. Thus, we identify that an entangled quantum memory, which is limited to record results of compatible POVMs, cannot assist in beating the entropic uncertainty bound. As a consequence, we show that the quantum advantage in ensuring security in key distribution against collective attacks is lost, even though a suitable entangled state is employed – but with the joint measurability constraint.
The effects of the entropic criteria of steering was formulated for position and momentum by S. P. Walborn, A. Salles, R. M. Gomes, F. Toscano, and P. H. Souto Ribeiro, Phys. Rev. Lett. 106, 130402 (2011). Entropic steering inequalities for discrete observables were developed more recently in Ref. [18].

S. T. Ali, C. Carmeli, T. Heinosaari, and A. Toigo, Found. Phys. 39, 593 (2009).

The first entropic criteria of steering was formulated for A. Fine, Phys. Rev. Lett. 48, 21 (1982); ibid., J. Math. Phys. 23, 1306 (1982).

The roles played by Alice and Bob in non-local steering task (where conventionally Alice is an untrusted party and Bob needs to check violation/nonviolation of a steering inequality to verify if Alice’s claim – that they share an entangled state – is true/false) is interchanged here so as to be consistent with the convention of Ref. [17].

H. Maassen and J. B. Uffink, Phys. Rev. Lett. 60, 1103 (1988).

M. Krishna and K. R. Parthasarathy, Sankhya 64, 842 (2002).

S. Wehner and A. Winter, New J. Phys. 12, 025009 (2010).

Note that $H(\mathcal{X}|\mathcal{X}') = - \sum_{x,x'} p(x|x') \log_2 p(x|x')$ – where $p(x,x') = \text{Tr}[\rho_{AB} E_{\mathcal{X}}(x) \otimes E_{\mathcal{X}'}(x')]$, $p(x|x') = \rho_{x|x'}$, $\rho_{x'|x} = E_{\mathcal{X}}(x|\mathcal{X}')$, $\rho_{x|\mathcal{X}'} = E_{\mathcal{X}'}(x)$ and $\rho_{x|x'}$ is the conditional Shannon entropy associated with the probabilities of Alice finding the outcome $x$ of the POVM $\mathcal{X}$, when Bob has obtained the outcome $x'$ of the POVM $\mathcal{X}'$ and $\rho_{x|x'} = \text{Tr}[\rho_{AB} E_{\mathcal{X}}(x) \otimes E_{\mathcal{X}'}(x')] = \sum_x p(x,x')$ is the probability of Bob’s outcome $x'$ in the measurement of $\mathcal{X}'$.

The entropic steering inequality (11) is violated when the unsharpness parameter $\eta > 0.78$ – whereas the POVMs of [8] are incompatible for $\eta > 1/\sqrt{2}$ $\approx$ 0.707. In order to obtain the necessary and sufficient condition that the the POVMs of [8] are useful for steering in the entire range of incompatibility $1/\sqrt{2} < \eta \leq 1$, either one has to examine the set of all pure entangled states for the task of steering or to develop an appropriate steering inequality to capture the efficacy of the incompatible measurements [14, 15]. For instance, we find that the two qubit maximally entangled state shared between Alice and Bob violates a linear steering inequality with two measurement settings (Eq. (64) of E. G. Cavalcanti, S. J. Jones, H. M. Wiseman, and M. D. Reid, Phys. Rev. A 80, 032112 (2009)) for the entire range of incompatibility $1/\sqrt{2} < \eta \leq 1$ of the unsharpness parameter, when Bob (who claims to steer Alice’s by measurements at his end) measures the pairs of POVMs of [8].

M. Tomamichel and R. Renner, Phys. Rev. Lett. 106, 110506 (2011).

J. M. Renes and J.-C. Boileau, Phys. Rev. Lett. 103, 020402 (2009).

P. J. Coles, L. Yu, V. Gheorghiu, and R. B. Griffiths, Phys. Rev. A 83, 062338 (2011).