Noise and Entropic Uncertainty Relations in Quantum Systems

A Thesis

submitted to

Indian Institute of Science Education and Research Pune in partial fulfilment of the requirements for the BS-MS Dual Degree Programme

by

Avik Mukherjee

Indian Institute of Science Education and Research Pune
Dr. Homi Bhabha Road,
Pashan, Pune 411008, INDIA.

July 2021
Supervisor: Dr Arun Kumar Pati
Avik Mukherjee

Certificate

This is to certify that this dissertation entitled Noise and entropic uncertainty relations in Quantum Systems is towards the partial fulfilment of the BS-MS dual degree programme at the Indian Institute of Science Education and Research, Pune represents study/work carried out by Avik Mukherjee at Indian Institute of Science Education and Research under the supervision of Dr Arun Kumar Pati, Professor, Department of Physics HRI, during the academic year 2020/2021

Arun Kumar Pati

Dr. Arun Kumar Pati

Dr T.S Mahesh

This thesis is dedicated to my father

Declaration

I hereby declare that the matter embodied in the report entitled Noise and Entropic Uncertainty Relations in Quantum Systems are the results of the work carried out by me at the Department of Physics, HRI, Prayagraj, under the supervision of Dr Arun Kumar Pati and the same has not been submitted elsewhere for any other degree

Avik Mukherjee

Date: 15.9.2021

Table of Content Page Number

Abstract

The laws of nature, in the Quantum domain is markedly different from the statistical laws that scientists have developed for classical systems in the field of thermodynamics or information theory. One of the main differences in the quantum domain is the presence of uncertainty relations, which ensures certain properties of a system cannot be fundamentally measured to arbitrary degrees of precision. Entropy is one of the most fundamental properties of quantum systems that gives these kinds of relations called Entropic Uncertainty Relations (EUR). These EURs provide a fundamental tool in the development of many Quantum Computing algorithms such as teleportation. In a world where Quantum Computing looks more and more promising to break the barriers of traditional computing, EUR proves to play a crucial role in developing and strengthening the protocols needed for the paradigm shift.
One of the main problems with the use of quantum technologies is that they are rarely robust in the presence of noise, while our immediate operative surroundings have a plethora of noise. So, it becomes increasingly important to study EURs in the presence of noisy channels. In this project we study the development of simple EURs and their behaviour in the presence of noise.

Acknowledgments

I want to thank IISER Pune and HRI for giving me the opportunity to work on this project. I am indebted to Dr Arun Kumar Pati for letting me join his course on Quantum Information and his guidance for the project. I would also like to thank my father for his support.

Introduction

Origins of Uncertainty Relations

During the developmental days of Quantum Mechanics, there was a major focus on the study of fundamental particles which were considered the building blocks of matter.

Therefore, given a Quantum system A comprising of individual particles, the most important properties that required measurements were Position(P) and Momentum (Q). So, it is not surprising that the very first uncertainty relation that was proposed was by Heisenberg, stating the inability to accurately predict the P and Q measurables of a system. This relation knowns as the Heisenberg Uncertainty Relation, was later mathematically formalized by the works of Kennard, E. H. (1927) who used the standard deviation approach to quantify the relation.

This formulation was further advanced by the works of Robertson[Robertson, H. P. (1929)], who gave a more general equation for standard deviation uncertainty relation (SDUR)
The Robertson SDUR for two general measurements A and B for any given system was derived as

$$\Delta A \, \Delta B \geq \frac{1}{2} | < [A, B] > |$$

Where ΔA gives the variance of the measurement operator A, while $[A, B]$ is the general commutator term for the measurements.

The major drawback of the the uncertainty relation mentioned above is that it shows marked dependence with the state of the system that we are measuring. So if the prepared state is an eigenstate of any of the two operators A, B then the right hand side of the equation is reduced to zero. That means the inequality becomes trivial and we get no fundamental knowledge about the measurement spread of the system.

A further improvement of the relation was done by the famous physicist Erwin Schrodinger (Schrödinger, E. (1930)) who added another state dependent anti commutator term which although strengthened the relation, did not overcome the main major defect mentioned above.

Improvement of the Standard Deviation Approach

The general form of the uncertainty relation derived through the standard deviation approach remained unchanged for a long period of time till Maccone and Pati (Maccone, L., and A. K. Pati (2014)) derived a stronger set of inequalities that were usable for a more general set of states. This uncertainty relation can be thought of as a combination of two separate uncertainty inequalities.

$$\Delta A^2 + \Delta B^2 \geq max(\beta_1 + \beta_2)$$

Where the separate inequalities are

$\beta_1 = \pm i<[A,B]> + |<\psi| A \pm iB |\psi^p>|$

$\beta_2 = \frac{1}{2}|<\psi^{po}| A \pm B |\psi>|^2$

Here the state ψ^p is defined as any state perpendicular to the state of ψ. Whereas ψ^{po} is another state of the form $|\psi^{po}>=(A+B-<A+B>)|\psi>$.

The advantages of using these particular inequalities along with their proof is discussed below.

Proof: Let us redefine two operators, C and D as the difference of A and B from their respective expectation values. We would use the parallelogram inequality which states that for two random vectors f and g on a Hilbert space H, the following inequality always holds.

$$\frac{||f - g||^2 + ||f + g||^2}{2} \leq ||f||^2 + ||g||^2$$

Replacing the vectors f and g with the vectors $C, \alpha D \; where \; \alpha \in \mathbb{C} \; ||\alpha|| = 1$ we get the inequality

$$||C + \alpha D||^2 + ||C - \alpha D||^2 = 2(\Delta A^2 + \Delta B^2)$$

Now from the definition of the operators C and D and replacing $\alpha = 1$ we get the equation

$$\Delta(A+B)^2 \leq 2(\Delta A^2 + \Delta B^2)$$

The LHS of the equation is equivalent to β_2.
Putting $\alpha = i$ we get the LHS of the equation equal to β_1, proving the EURs.

The RHS of this SDUR is markedly different from the previously proposed SDUR, because these do not give trivial results when the state is an eigenstate of either of the measurement operators. But this does still, give a trivial result when the state is an eigenstate of the summation of the observables in question.

Irrespective of state dependence, the standard deviation approach to Uncertainty relations led to some fundamental questions on whether it was the best possible measure of uncertainty in Quantum systems. The root cause for the dispute was the counter intuitive behaviour of the standard deviation function when applied to simple systems, which we will discuss in the next section.

Problems with Standard Deviation

While measuring the uncertainty in Quantum Systems there were multiple major issues that scientists faced with. One of them was the fact that not all systems had a related uncertainty that could be assigned a numerical significance. One of the most prominent example is that of neutrinos, where the flavour of the neutrino can be modelled as a probabilistic event with different end results. It is not possible to assign a standard deviation to such systems, but the system still can have the concept of uncertainty.

The other main issue with the standard deviation as a measure of uncertainty was captured by Rudnicki [Rudnicki, Ł., Z. Puchała, and K. Życzkowski (2014)]. A simple example would be to imagine two small boxes in which a particle may be located separated by a large distance L. There is no correlation between the probabilities associated with the two boxes. On further separation of the boxes the uncertainty of the system should not vary according to our common sense, while the standard deviation as a measure is found to be proportional to the distance between the two boxes.

This highlights that the standard deviation is extremely biased toward values which are further away from the mean of the spread and hence does not give an accurate representation of the finer structures of the distribution.

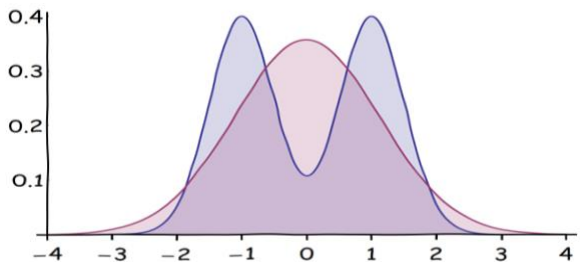


Fig: Unimodal and Bimodal distributions with same Std Dev

For example, the difference between a unimodal distribution and bimodal distribution like the blue and red curves above is not expressed through the standard deviation model.

Due to these major issues, scientists proposed entropy as a more suitable quantity as a measure of uncertainty. According to the work of Friedland and Gour [Friedland, S., V. Gheorghiu, and G. Gour (2013)], the two major properties of a good measure for uncertainty are:

- The uncertainty of a system cannot decrease under random relabelling of the coordinates. This is another property that is not followed if we use standard deviation as our chosen measure.
- The uncertainty of a system cannot decrease if a subsystem containing information to the system is lost.

These two major properties are followed by Shannon and Von Neumann entropy, which makes them better candidates as a measure for uncertainty.

The language of entropy also enables us to borrow ideas and theorems already established in the field of information theory. These come handy in the use of data compression or quantum key distribution as discussed later. This brought up the idea of Entropic Uncertainty Relations as discussed in the next section.

Entropic Uncertainty Relations (EUR)

The concept of information was first linked to entropy by Claude Shannon in his seminal work of 1948 [Shannon, C. (1948), Bell System Technical Journa]. He argued that any event that has a probabilistic spread of outcomes can be deemed to have an information content. The information content of the event is strictly determined by the probability distribution and not by the numerical values of the outcomes themselves. For an example we take the event of tossing a coin. If we consider this as an event which has two distinct outcomes, the coin landing on its face and the coin landing on its side. It is obviously highly more probable that the coin would land on it' face and not on the side. Thus the information content from that event would be minimal, as we would already know what the possible outcome would be. Whereas, if the two possible outcomes of the event were the coin landing tails up or heads up, the probability of them would be almost equal. In that case the information content of the even would be higher, since we have little hope of guessing what the possible outcome of one realisation of the event would be.

Therefore for an event with outcome space $X = \{x_1, x_2, x_n\}$ and Probability distribution $P(X) = \{p_1, p_2, p_n\}$ we needed a measure for quantifying uncertainty which would satisfy the following properties:

- The measure would depend on the set $P(X)$ and not on the set X.
- The measure would be minimised when the event was certain, which means $p_k = 1 \; for \; some \; k \; , p_n = 0 \; for \; all \; other \; n$
- If the outcomes set can be fragmented into successive outcome sets, then the measure would be the weighted sum of the measure of the successive outcomes.
- The measure is continuous on the event outcome space.

The function that allows all three above properties is known as the Shannon Entropy and is defined as

$$H(X) = -\sum P(x) log P(x)$$

Although there were different other forms of entropies and uncertainty relations associated with them, we would mostly focus on Shannon Entropy and it's quantum counterpart the Von Neumann Entropy in the context of EUR.

Von Neumann Entropy

The Von Neumann Entropy is the extension of the Shannon Entropy for Quantum Systems. The mathematical expression for this is

$$H(\rho) = -Tr(\rho \ln(\rho))$$

Where ρ is the density matrix of the system.

A basis change in Quantum Mechanics can be represented with an unitary transformation U. But $H(\rho)$ is invariant under the transformations of the form

$$\rho \underset{u}{\rightarrow} U'\rho U$$

This is an important property of a desirable uncertainty measure as we have mentioned before.
The Von Neumann entropy is minimal for a pure state and maximizes for a maximally mixed state.
It also captures the inherent uncertainty of quantum systems, unlike Shannon entropy. For example, a system comprising of a collection of two spin half particles in thez_+ state and x_+ state, would give a Shannon entropy of 1. While the Von Neumann entropy calculated from the corresponding density matrix is different.

Development of EUR

One of the first EUR, was due to the work by Maassen and Uffink (Maassen, H., and J. Uffink (1988)) who improved on the work of Deutsch and gave the following Uncertainty Relation for a system A, and observables P and Q

$$H(P) + H(Q) \geq -log\, c$$

Where *c* is the maximum overlap function of the two observables defined by

$$c = max\, c_{xz} \;\; and\; c_{xz} = |<P|Q>|^2$$

The major benefit of the Maassen Uffink EUR is that unlike the standard deviation based approach, here the inequality is not dependent on the state of preparation of the system A. From the equation it is evident that the inequality becomes trivial when the two measurement bases have a common vector as the value of c becomes unity.

The other extreme end is when the two measurements are mutually unbiased. This is defined as when knowledge about one measurement implies zero knowledge about the other. Two bases are said to be mutually unbiased when they follow the relation:

$$|<P|Q>|^2 = \frac{1}{d}$$

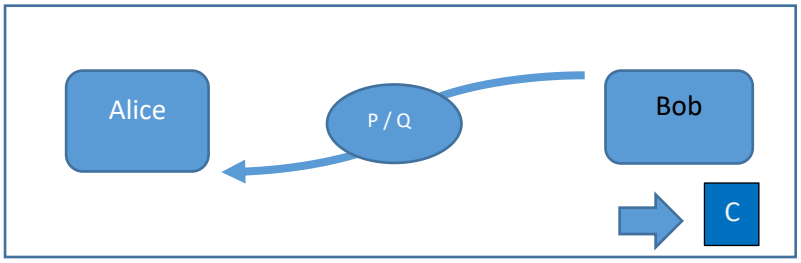
Here *d* is the dimension of the associated Hilbert space.

Now to use this in the context of quantum information we needed to reform the above ideas in the context of a guessing game, which is the preferred setting in many problems of information theory. A guessing game is usually played by two or more players where one performs some operation on the system of which the other player has incomplete knowledge of. The idea is to find an optimal strategy for the second player to guess the outcome.

In the context of EUR, we consider a two player game between Alice and Bob who have access to a system *A* in state ρ_A. Bob performs either *P* or *Q* measurement on the system and gets an outcome C.

Now he sends back to Alice his choice of measurement. The game is to find the optimal probability that Alice has of guessing the measurement outcome C.

Fig : In this particular game, Bob has an outcome C that Alice has to guess, given the choice of measurement



Using the Massen Uffink EUR on the conditional probability distribution and dividing both sides by 2 we get the relation

$$\frac{H(K|P) + H(K|Q)}{2} \geq \frac{q_{MU}}{2}$$

Now because of the property of entropy we can consider the event as choosing either of the measurement with probability $\frac{1}{2}$ and then condition the entropy on the chosen measurement

$$H(K|P,Q) = \frac{H(K|P) + H(K|Q)}{2}$$

So we infer that $H(K|P,Q) \geq \frac{q_{MU}}{2}$ which implies that the probability of Alice guessing the outcome is non zero as long as the maximum overlap function is non zero.

Tighter inequalities have been developed based on this guessing game by Schaffner[Schaffner, C. (2007)] who related the minimum and binary entropy of the observables to the probability of winning the guessing game.

It is important to be noted that all the EUR discussed are by definition, preparation uncertainty relation, which means the fundamental uncertainty is not caused due to some local disturbances caused by measurements. There is another class of measurement uncertainty relations which we have not discussed here.
The main drawback of the Maassen Uffink EUR was that it was not a tight EUR, so there were many attempts that were further introduced to improve upon the bounds of the inequality. Two such approaches were the majorization approach and the assisted memory approach.

One important aspect of the EUR that we have discussed till now is that they do not deploy the use of classical or quantum memory. In the context of our guessing games a memory can be thought of as any system that has ancillary knowledge which can be used to guess the influence of the player. The information itself can be classical or quantum, both of which we will investigate.

Memory assisted EUR

Conditional Entropy

The conditional entropy of a bipartite system ρ_{AB}, conditioned on B is given by

$$H(A\,|\,B) = H(AB) - H(B)$$

It is a good measure of the uncertainty in A when B is given.

For a classical system the conditional entropy is always positive, but the same cannot be said about quantum systems. Cerf and Adami [N. J. Cerf, C. Adami, 1997] proved that for systems showing entanglement the conditional entropy can take on negative values. Negative values of $H(A\,|\,B)$ is a sufficient but unnecessary condition for entanglement.

Classical and Quantum Memory

The presence of a memory for Alice, can help improve the guessing probability. Imagine a simple system quantum system prepared in state x_i , where all x_i are mutually orthogonal, depending on the roll of dice d_i. Now for joint state $\rho_{xd} = \sum x_i\ d_i$, if Bob has the access to the classical dice, then he can with certainty guess the state x_i. This shows, that classical memory can help improve the probability of guessing. The limitation for a classical memory is, that with if Alice does the measurement in some other basis complementary to X, the knowledge of the classical memory doesn't help improve the guessing probability.
For a quantum state ρ_x, and classical memory Y we have the conditional entropy.

$$H(X|Y)\ = \sum_y P(y)H(X\,|Y = y)$$

Now, from Maassen Uffink EUR we know, for a set of measurements X_n we have the EUR

$$\sum_n H(X_n) \geq\ q$$

Where the term q is independent of initial preparation. Now, since this EUR applies for all quantum states, it also holds for states where $Y = y$ in the classical memory. Therefore

$$\sum_y P(y) \sum_n H(X_n \,|Y = y) \geq \; q$$

Which is the extension of the EUR, in the presence of classical memory.

In the presence of a quantum memory, we can think of our previous guessing game as Alice preparing a system with a quantum memory that she retains with herself. Bob performs the measurement and sends her, the choice of measurement. Let us take the example of a Bell state of the form

$|\Psi >= \frac{|0>|1>+|1>|0>}{\sqrt{2}}$. Here one can think of the second qubit to be quantum memory that Alice retains while the first qubit is sent to Bob. Now after Bob has made his measurement and communicated his choice, Alice can with probability 1 guess the outcome of the measurement.

This shows that the presence of quantum entanglement between the memory and the system has effect on the EUR. So it is natural that any EUR would have a term quantifying the amount of the corelation between the system and the memory. This conjecture was proved by Christandl and Berta [Berta, M., M. Christandl, R. Colbeck, J. M. Renes, and R. Renner (2010)] who gave the modified EUR in presence of quantum memory for a compound state ρ_{AB} with B being the quantum memory as

$$H(Y|B) \; + H(X|B) \; \geq \; q_{XY} + H(A|B)$$

We see that the value of $H(A|B)$ = -log *d,* when the memory is maximally entangled. Since the overlap function q_{XY} also has the maximum value of log d, we see the RHS reduces to zero as in our previous example.
While, if the memory B and A are not corelated at all, the extra term goes to zero and we retrieve our original Maassen Uffink EUR. This improvement comes at the cost that now the EUR is again dependent on the state of the system as the term $H(A|B)$ is state dependent.

Further improvement on the bounds of memory assisted EUR was done recently by Pati [Pati, A. K., M. M. Wilde, A. R. U. Devi (2012)].

Their main argument was that classical correlations and quantum discord of a system can be effectively used to further tighten the inequalities.
For a composite system state ρ_{AB} the mutual information of the two subsystems A and B is defined as

$$I(\rho_{A:B}) = S(\rho_A) + S(\rho_B) - S(\rho_{AB})$$

This is a measure of the total correlations of the compound system AB. The classical correlation of the compound system is defined by

$$J_A(\rho_{AB}) = max_X\, I(X:B)$$

Where the maximisation is done over all possible POVM measurements on the system A. The measure of the quantum corelations between the two subsystems can be expressed as the difference between the classical correlation and the mutual information.

$$D_A(\rho_{AB}) \equiv I(A:B) - J_A(\rho_{AB})$$

This quantity is called quantum discord. The EUR proposed by Pati et.al relates the quantum discord and the classical correlations to the conditional entropy by

$$H(X|Y) + H(X|B) \geq\ q_{XY} + H(A|B) + D_A(\rho_{AB}) - J_A(\rho_{AB})$$

The proof of this relation has been added in Appendix A.

Effect of Noise on EUR

In practicality most Quantum Systems are never completely isolated from the environment. The effective noise on the quantum systems can be due to multiple reasons, like thermal noise or faulty quantum channel. Therefore, there is a need to explore the behaviour of the Entropic Uncertainty Relations in presence of various kinds of noisy channel.

Noise is modelled in quantum information as Kraus operators. For any quantum operation Ω on a state ρ , we can express the effect of the operation as

$$\Omega(\rho) = \sum_i K_i{}^* \rho K_i$$

Where the K_i are called the Kraus matrices of the corresponding operation if they follow the condition $\sum_i K_i{}^* K_i = 1$.

In Quantum information theory, these operators are also called noise operators because they are used to introduce noise into the system.

Let us modify the guessing game introduced earlier to show the effect of noise.

1. Alice prepares a compound state ρ_{AB} with a quantum memory B and sends it to Bob.
2. The Quantum memory B is free from any error, while the system A, experiences some noise.
3. Bob makes a measurement in one of two basis σi or σj and sends the choice of measurement back to Alice again through a classical noise less channel.
4. Alice has to guess the measurement outcome with the help of memory B and the received choice of the measurement basis.

The noise induced can be of any form in our noise channels. But let us focus on few of the more simpler noise channels in Quantum Information.

Bit Flip channel: The bit flip is a noise channel that flips the two bases based on some probability p.

$$B(\rho) = (1-p)\rho + pX\rho X$$

Phase shift channel: This channel changes the relative phases of the state. That is $\alpha|0> +\beta|1> \xrightarrow{P} \alpha|0> -\beta|1>$. The representation for this channel is

$$P(\rho) = (1-p)\rho + pZ\rho Z$$

Phase and bit shift channel: This channel changes both the relative phase and flips the bit with some probability p.

$$BP(\rho) = (1-p)\rho + pY\rho Y$$

Effect of noise on Maassen Uffink EUR

The effect of these quantum noise channels on the Massen Uffink EUR was investigated by [Xu et al. 2010]

The best initial choice of the state of the system is to prepare it in the Bell Diagonal state, which are states that can be expressed as the convex combination of the Bell states.
The general form of a Bell diagonal state is given by

$$\rho_{bd} = \nu_1|\psi^+><\psi^+| + \nu_2|\phi><\phi^+| + \nu_3|\psi^-><\psi^-| + \nu_4|\phi^-><\phi^-|$$

Let the compound state created by Alice in one such state. The state can be expressed in the form $\frac{\mathbb{I}^A \otimes \mathbb{I}^B + \sum_j^{j<3} C_{\sigma j}(\sigma_j{}^A \otimes \sigma_j{}^B)}{4}$

Where the $C_{\sigma j}$ are related to the eigenvalues of the Bell states ν_i.
There are major advantages of creating the initial state in Bell Diagonal state. Few of the properties of them are:

- The state is completely separable if all of the eigenvalues ν_i is less than 0.5
- Subsystems of 2 qubit bell diagonal states are maximally mixed. [Quantum Information, M Wilde].
- The space of the Bell diagonal states can be visualised as a tetrahedron with the diagonal elements as the $C_{\sigma j}$.

Given that the state is initially prepared in a bell diagonal form, we will try and find the condition that it hits the lower bound in the Maassen Uffink EUR.

After the measurement of the qubit A in σ_x, the conditional entropy of the state becomes

$$H(\sigma_x|B) = H_{bin}(\frac{1 + C_{\sigma_x}}{2})$$

Similarly for σ_y we have

$$H(\sigma_y|B) = H_{bin}(\frac{1 + C_{\sigma_y}}{2})$$

Where H_{bin} is the binary entropy function given by H(p)=–(1-p)$\log_2(1-p)$-p$\log_2(p)$. [M. A. Nielsen and I. L. Chuang 2000).].

The c value for any pair of Pauli matrices would be 0.5.

Now the RHS of the Maassen Uffink uncertainty relation is

$-\log_2(c) + H(A|B)$

≈ 1 + $H(AB)$-$H(B)$

≈ 1 + $H(AB)$-1
Where we have used the property of the Bell diagonal states that the subsystems of 2 qubit states are maximally mixed.

≈ $H(AB)$

By the expansion of Shannon entropy this can be written as

$\approx -\sum_i v_i \log_2(v_i)$

This equals the RHS of the Maassen Uffink inequality $H_{bin}(\frac{1+C_{\sigma_y}}{2})$ + $H_{bin}(\frac{1+C_{\sigma_x}}{2})$ for a special combination of v_i. Mapping that to the corresponding C_{σ_i}, the bound is only satisfied for the special set of condition

$$C_{\sigma_i} = -C_{\sigma_j} * C_{\sigma_k}$$

Xu describes this condition as SPMC condition of state preparation under which the lower bound of the EUR is reached.

When the first qubit is passed through the noisy channel, we assume one of the three noise channel acts on it. Then the coefficients of the new state D_{σ_i} are mapped to old C_{σ_i} as

$$C_{\sigma_i} = D_{\sigma_i}$$

$$D_{\sigma_m} = (1-2p)D_{\sigma_m}$$

Where *p* is the probability of the error channel acting on the state.

Now the condition of D_{σ_m} satisfying the SPMC condition after going through the noisy channel is given by

$$D_{\sigma_i} = -(1-2p)^2 D_{\sigma_j} D_{\sigma_k}$$

Given that p is a small number less than 1, this is only satisfied by the condition that p = 0. So the lower bound for measurement $\sigma_y\sigma_z$ is reachable when the σ_x noise or the bit flip noise is not present. The same argument holds for all other pairs of the Pauli matrices.

Huang et. al [], has also shown that for unital noise channels such as the bitflip phase flip and bit phase flip, the EUR increases and gradually flattens off with time. This is in line with our intuition that with time, the quantum correlations would gradually decrease, increasing the measurement spread.

But in the presence of non unital noise such as the amplitude damping channel, it has been shown that the behaviour of the EUR is markedly different. On tweaking the nature of the noise, it is possible to bring the entropy even lower than the bound predicted by the Maassen Uffink EUR.

Conclusion and Discussion

From this project I have learnt about the historical development of Uncertainty relations from standard deviation approach to entropic approach. Then we focused effect of additional quantum and classical memory on the Maassen Uffink EUR to strengthen the bounds of the inequality. The cause for this effect is the quantum entanglement between the memory and the system which leads to negative relative conditional entropy. The motivation to study Entropic Uncertainty principles come because they find usage in areas of Quantum Randomness generator and Entanglement Witness.

Quantum Randomness: Randomness as a mathematical tool is used in many scientific models ranging from cryptography to micro finance. But due to the deterministic structure of the generator used in most cases, the resultant quantity is often mostly pseudorandom. Quantum Mechanics, due to its inherent uncertainty, lays the path to the production of information theoretically secure random numbers.
Entropy can be thought of as a measure of randomness, and providing lowering bounds of measurement entropy through EUR can help quantify randomness.

Entanglement Witness: Entanglement is one of the uniquely special properties of a quantum system, and hence the study and measurement of entanglement becomes a part of quantum information processing. Entanglement witness refers to the ability of identify if the particles being emitted from a source are entangled or separable. This is usually achieved through identifying a relation that is satisfied for separable states and then showing that the particle source violates the relation. (Berta et al. (2010)) Entropic relations are useful in this context, because as we have seen, the entanglement measure and quantum discord are linked to the EUR. So, measurement of the spread of the outcomes often gives us an indication of the presence of entanglement between system and memory.

Appendix A

Proof of the relation

$$H(Y|B) + H(X|B) \geq q_{XY} + H(A|B) + D_A(\rho_{AB}) - J_A(\rho_{AB})$$

Taking the LHS of the equation

$> H(Y|B) + H(X|B) = H(XB) + H(YB) - H(B) - H(B) - H(X|B)$

$> H(Y|B) + H(X|B) = H(X) + H(Y) - I(\rho_{X:B}) - I(\rho_{Y:B})$

This follows from the definition of $I(\rho_{Y:B})$

$> H(X|Y) + H(X|B) \geq H(X) + H(Y) - 2J_A(\rho_{AB})$

This inequality follows from the fact that X and Y are not the maximising observables on J.

$> H(X|Y) + H(X|B) \geq q_{XY} + H(A) - 2J_A(\rho_{AB})$

Using the Maassen Uffink EUR

$> H(X|Y) + H(X|B) \geq q_{XY} + H(A|B) + D_A(\rho_{AB}) - J_A(\rho_{AB})$

The last relation follows from the definition of Quantum discord as

$$D_A(\rho_{AB}) \equiv I(A:B) - J_A(\rho_{AB})$$

Whenever the quantity $D_A(\rho_{AB}) - J_A(\rho_{AB})$ is higher than zero, we get a stronger EUR than the basic Maassen Uffink EUR. Together, the complete EUR is

$$H(Y|B) + H(X|B) \geq q_{XY} + H(A|B) + \max(0, D_A(\rho_{AB}) - J_A(\rho_{AB}))$$

References

Berta, M., M. Christandl, R. Colbeck, J. M. Renes, and R. Renner (2010), Nature Physics 6 (9), 659.

Berta, M., P. J. Coles, and S. Wehner (2014a), Physical Review A 90 (6), 062127

Białynicki-Birula, I. (1984), Physics Letters A 103 (5), 253

Friedland, S., V. Gheorghiu, and G. Gour (2013), Physical Review Letters 111 (23), 230401.

Huang, A.-J., Shi, J.-D., Wang, D., & Ye, L. (2016). Quantum Information Processing, 16(2).

Kennard, E. H. (1927), Zeitschrift für Physik 44 (4-5), 326

Maassen, H., and J. Uffink (1988), Physical Review Letters 60 (12), 1103.

M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information (Cambridge University Press, Cambridge, England, 2000).

Maccone, L., and A. K. Pati (2014), Physical Review Letters 113 (26), 260401

Pati, A. K., M. M. Wilde, A. R. U. Devi, A. K. Rajagopal, and Sudha (2012), Physical Review A 86 (4), 042105.

Robertson, H. P. (1929), Physical Review 34 (1), 163.

Schaffner, C. (2007), Cryptography in the Bounded-QuantumStorage Model, Phd thesis (University of Aarhus).

Schrödinger, E. (1930), Proceedings of the Prussian Academy of Sciences XIX, 296.

Shannon, C. (1948), Bell System Technical Journal 27, 379.

Z. Y. Xu, W. L. Yang, and M. Feng Phys. Rev. A 86, 012113