Entropic Uncertainty Relations

A Major Qualifying Project Submitted to the Faculty of

Worcester Polytechnic Institute

In partial fulfillment of the requirements for the Degree in Bachelor of Science in Physics

By
Nicholas Richard Marshall

Date
May 4, 2021

Advisors
Professor Padmanabhan Aravind
Professor Herman Servatius

Abstract

The intent of this MQP is to discuss the notion of Entropic Uncertainty Relations (EUR). The advantage of EUR over the Heisenberg and Robertson uncertainty relations, which are discussed in most quantum texts, will be discussed. Examples of the relations will be described mathematically and graphically for 2- and 3-dimensional quantum systems (qubits and qutrits). These relations are of interest in the development of quantum cryptography, particularly in guaranteeing security in key distribution schemes.

Acknowledgements

A special thank you to Professor Aravind for guiding me through quantum information over the course of my Junior year in preparation for a final MQP project and taking me on as my advisor for the proceeding MQP.

Thanks to my parents to supporting me throughout my time at Worcester Polytechnic Institute in every way they can.

Contents

Introduction

Of all the ideas underlying quantum mechanics, the most well-known relation, in both core texts and pop culture, is the Heisenberg uncertainty relation [1]. This relation states that there is a limit to how precisely one can simultaneously determine both the position and momentum of a particle in a given quantum state. It does this by showing that the product of the position and momentum uncertainties must always exceed a certain minimum value. An important feature of quantum mechanics, reflected in the uncertainty principle, is that a measurement on a quantum system can cause disturbances to it, i.e., change its properties in an unpredictable way. Heisenberg's uncertainty relation was later generalized by Robertson to include any two non-commuting observables [1]. The expanded scope of the Robertson uncertainty principle makes it applicable to a much wider range of problems than the Heisenberg relation, and it has been used to analyze the limits imposed by quantum mechanics on the operation of all sorts of devices.

In a parallel and unrelated development, Claude Shannon of Bell Labs developed the fundamental ideas of information theory in the 1940s [2]. He introduced a fundamental concept, known as the Shannon entropy, that can be used to quantify the amount of information in any bank of data, such as a music CD or a personal computer. The value of Shannon's theorems is that they allow us to determine the resources needed to encode and transmit information effectively, even in the presence of noisy channels.

In 1980 Maassen and Uffink [4] used the notion of Shannon entropy to quantify the uncertainty of observables in a quantum state, and they were thereby led to a new type of uncertainty relation known as the Entropic Uncertainty Relations (EUR). The term EUR is now used to refer to a whole family of relations that all generalize the original relation of Maassen and Uffink in a variety of ways. These new relations are more powerful than the conventional uncertainty relations for the analysis of many problems, including ones in quantum information theory.

In 1984, well before the advent of quantum computing, Bennett and Brassard [5] proposed a secret key distribution scheme based on two-state systems or qubits. Their scheme involved using the polarization states of photons to transmit and generate the key. The novelty of their scheme was that its security is guaranteed by the laws of quantum mechanics. This makes it very different from classical encryption schemes, whose safety relies upon the near impossibility of a mathematical task that must be performed by an eavesdropper to break the key.

However, the safety of the scheme is more involved than may be gathered from the preceding remarks. A clever eavesdropper can intercept the quantum particles and therefore gain partial information about the key being generated by the two parties. The way the legitimate users can counter this threat is to use a suitable form of the EUR to infer the amount of information that has leaked away to the eavesdropper. They can then take corrective steps to ensure that the useful information possessed by the eavesdropper is made as close to zero as desired. Because of the importance of EURs to quantum cryptography, it was chosen as the focus of this project.

In this report the Heisenberg and Robertson uncertainty principles will first be discussed, and their limitations will be pointed out. The notion of Shannon entropy will then be introduced and some examples of it will be given. Then the simplest EURs for two-state systems (or qubits) and three-state systems (or qutrits) will be introduced and illustrated by means of some basic calculations. Finally, it will be pointed out how the EURs studied in this project need to be generalized to make them relevant to the analysis of security in quantum key distribution schemes.

Chapter 1

Heisenberg Uncertainty Principle

The relation that describes how precisely one can simultaneously determine the position and momentum of a particle is the Heisenberg Uncertainty Principle. It is described, for example, in the text by Schumacher and Westmoreland [6]. It was originally discovered by Heisenberg before a more general relation that provides a similar result for any two non-commuting observables. The Heisenberg relation provides a lower limit to the product of the standard deviations of the position and momentum observables. If Q and P are the position and momentum observables, and $\sigma(Q)$ and $\sigma(P)$ are their standard deviations, then

$$\sigma(Q) \cdot \sigma(P) \geq {}^{\hbar}\!/_{2} = {}^{h}\!/_{4\pi} \quad (1.1)$$

This is one of the most commonly known relations in quantum mechanics, if even just by name. It is taught early on as it demonstrates how certain quantum measurements are not independent of each other but where the precision of one may disturb the precision of another. This result can be appreciated qualitatively by means of the following argument originally suggested by Heisenberg. To measure the position accurately one might decide to scatter a lower wavelength photon off it which will provide higher spatial resolutions. However, a low wavelength photon also has a high momentum and can impart some of its momentum to the particle thereby resulting in a greater error in the measurement of its momentum [6]. Conversely, if one uses a low frequency photon to minimize the error in the momentum measurement, the longer wavelength will lead to an inaccuracy in the measurement of the particle's position. It is this tradeoff between the accuracy of the two measurements that is captured by the principle.

We now introduce the definitions of some quantities that will be needed in the discussion below. If A is an observable and a quantum system is in the state ψ, the average value and standard deviation of the observable in the state are given by the equations

Expectation Value: $\langle \Psi | A | \Psi \rangle$ (1.2)

Standard Deviation: $\sigma(A) = \Delta(A) = \sqrt{\langle A^2 \rangle - \langle A \rangle^2}$ (1.3)

Here standard deviation is defined similarly to the way it is in statistics, but instead of using averages it uses the expectation value of an operator, A. In quantum mechanics expectation values refer to the average result one would measure on performing a large number of measurements on a specific state. The average need not equal the actual value (an eigenvalue) that one would find in any measurement. The standard deviation would then be computed from the data obtained in a large number of such trials.

The graph below plots the uncertainty of momentum on, the vertical axis, versus the position uncertainty, on the horizontal axis, for a minimum uncertainty state. The complementary nature of the asymptotes is made clear by the relation since as one tends to zero the other tends to infinity.

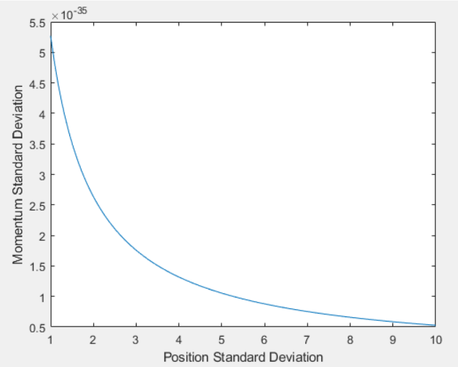


Fig. 1 Minimum uncertainty product as per Heisenberg Uncertainty Relation. Here the hyperbolic curve shows the drastic changes in the minimum standard deviation values with respect to each other.

While this is an important and basic result, it is still not an effective tool for applications in quantum information. The reason is that it is not possible to learn from it how much information can be stored in a variable utilizing position or momentum as a store for information. This shortfall makes it of limited value in problems connected with information storage and retrieval. None of this is to say the relation is not important. It still demonstrates fundamental limitations on what we can know and is an effective introduction to the idea of uncertainty principles.

When finding the product of these uncertainties there is a well-known case where the minimum uncertainty product is achieved. This case is for a wavefunction in the form of a Gaussian distribution. This case is discussed in many quantum texts such as Griffiths introduction to quantum mechanics [3]. However, the time evolution of a Gaussian state generally leads to a new state that is not a minimum uncertainty state, but rather one whose uncertainty product grows with time.

Robertson Uncertainty Principle

While Heisenberg was able to describe limitations on position and momentum measurements, Robertson was able to go further and describes limitations on any two non-commuting observables being measured simultaneously. His relation also differs from the Heisenberg relation in that it describes how the precision of the measurements is influenced by the particular state being measured [6].

Here we consider X, Y, and Z, which are the Pauli observables of a qubit. They represent measurements of the spin aligned with the X, Y, and Z axes in units of $\hbar/_2$ and can be represented by the 2x2 matrices.

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad (1.4)$$

Once more this principle allows a lower limit to be calculated for the product of uncertainties of the observables. This lower limit need not be the one that is observed in any set of experiments, but it can never be violated. The Robertson uncertainty principle is expressed in the equation

$$\sigma(X) \cdot \sigma(Z) \geq \langle \psi | [X, Z] | \psi \rangle \text{ (1.5)}$$

The left-hand side is the same as in the Heisenberg Uncertainty Principle in that it is the product of standard deviations. These standard deviations can be of any two non-commuting observables, but in the case the observables X and Z are used for spin-1/2 particles [6]. The right-hand side is the average of the commutator of the two observables in the state being considered. Standard deviation and expectation values are still defined the same way.

Examples

For this example, the Pauli observables X and Z will be used to demonstrate the lower limits given by the Robertson Uncertainty Principle.

Given:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad (1.6)$$

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad (1.7)$$

$$|\psi\rangle = \cos\theta \, | \, {}^{1}/_{2} \rangle + \sin\theta \, | -{}^{1}/_{2} \rangle = \begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix} \quad (1.8)$$

$$\sigma(x) = \sqrt{\langle X^2 \rangle - \langle X \rangle^2} \quad (1.9)$$

$$\langle X^2\rangle = \langle\psi|X^2|\psi\rangle = 1, \quad because\ X^2 = 1 \tag{1.10}$$

$$\langle X\rangle^2 = \langle\psi|X|\psi\rangle^2 = (2\sin\theta\cos\theta)^2 = (\sin 2\theta)^2 \tag{1.11}$$

$$\sigma(x) = \sqrt{1-\sin^2 2\theta} = |\cos 2\theta| \tag{1.12}$$

$$\sigma(Z) = \sqrt{\langle Z^2\rangle - \langle Z\rangle^2} \tag{1.13}$$

$$\langle Z^2\rangle = \langle\psi|Z^2|\psi\rangle = 1, \quad because\ Z^2 = 1 \tag{1.14}$$

$$\langle Z\rangle^2 = \langle\psi|Z|\psi\rangle^2 = (\cos^2\theta - \sin^2\theta)^2 = (\cos 2\theta)^2 \tag{1.15}$$

$$\sigma(Z) = \sqrt{1-\cos^2 2\theta} = |\sin 2\theta| \tag{1.16}$$

$$\sigma(x)\cdot\sigma(Z) = \cos 2\theta \sin 2\theta = {}^1\!/_2\,|\sin 4\theta| \tag{1.17}$$

$$\langle\psi|[X,Z]|\psi\rangle \tag{1.18}$$

$$[X,Z] = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix} - \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} = \begin{pmatrix}0 & -2\\ 2 & 0\end{pmatrix} \tag{1.19}$$

$$\langle\psi|[X,Z]|\psi\rangle = 2\sin\theta\cos\theta - 2\sin\theta\cos\theta = 0 \tag{1.20}$$

$$\sigma(X)\cdot\sigma(Z) \geq \langle\psi|[X,Z]|\psi\rangle \rightarrow {}^1\!/_2\,|\sin 4\theta| \geq 0 \tag{1.21}$$

Graphs

Shown below are graphs of the standard deviations $\sigma(X)$, $\sigma(Z)$ and their uncertainty product.

$\sigma(X)$ versus ψ

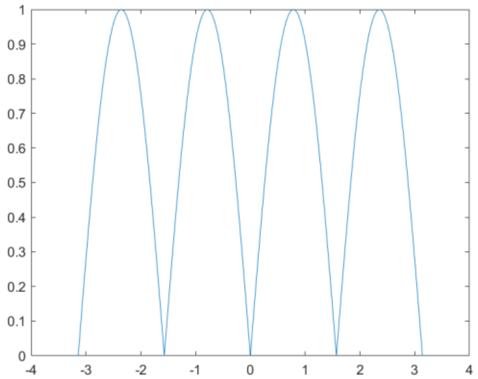


Fig. 1.2 Plot of how the standard deviation of X varies with the input state ψ. The curve shows how the standard deviation changes drastically over a period of π/2

$\sigma(Z)$ versus ψ

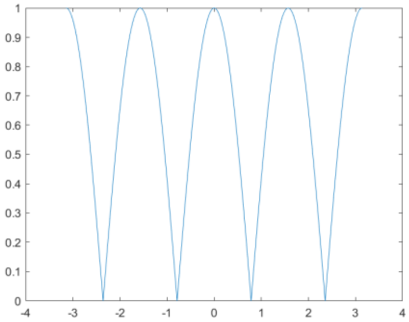


Fig. 1.3 Shows how the standard deviation of Z varies with the input state ψ. The graph shows it is the same result as for the standard deviation of X, but with a π/4 phase shift.

$\sigma(X) \cdot \sigma(Z)$ versus ψ

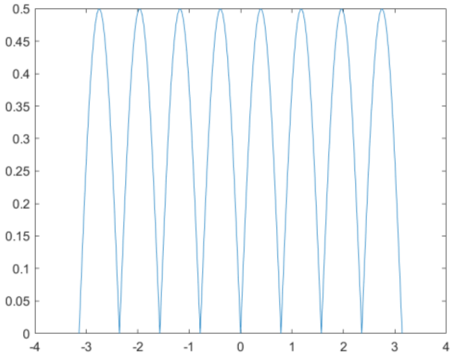


Fig. 1.4 demonstrates that the lower bound provided by the Robertson Uncertainty Principle is obeyed and the relation is saturated as it achieves equality when touching the ψ axis.

Combination of the above graphs

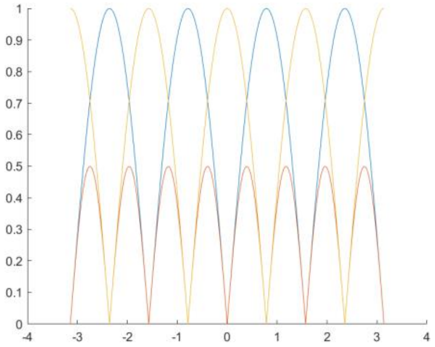


Fig. 1.5 allows one to more easily compare the values of the different graphs

From the last graph showing the product of uncertainties in the two observables, one can see that the Robertson Uncertainty Principle becomes an equality for multiples of $^{\pi}/_{4}$. When an uncertainty principle achieves equality it is said to have become saturated. This indicates that the lower bound it provides for the uncertainty product is achieved. If an uncertainty principle does not achieve equality then it is unsaturated and far less powerful. The unsaturated ucertainty is not the greatest lower bound possible, which would imply another uncertainty principle could provide an even greater lower bound and achieve saturation.

Both of these uncertainty principles can be found in many texts such as Schumacher and Westmoreland's *Quantum Processes Systems, and Information* [6], or the *Introduction to quantum mechanics* texts by Griffiths [3].

Chapter 2

Shannon Entropy

Shannon entropy is an important measure in information theory. The Shannon entropy of a system characterizes the surprise of a random variable and is related to the information content of its outcome. For an outcome that is guaranteed to occur there is no information gained in its measure, but for outcomes that are very unlikely there can be a much larger information content. Shannon entropy defines the average information content of some random variable [1].

$$H(X) = -\sum P_X(x) \log P_X(x) \quad (2.1)$$

As can be observed from the equation, an event that always occurs will have a Shannon entropy of zero as the logarithm vanishes. It is interesting to note that in attempting to maximize Shannon entropy, one should give every outcome an equal probability.

In information theory, entropy is important for describing how many bits are necessary to contain all the information of some data. This helps in compression as given some information you can find the minimum number of bits that are required to send information. One can use the Shannon entropy to quantify the information contained in quantum states and thereby be in a better position to explore issues related to the security of the quantum key distribution schemes [1].

H(X) Versus P(x_1)

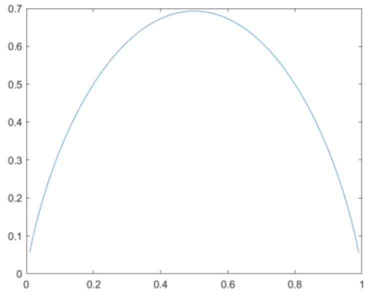


Fig. 2.1 Plots all possible Shannon entropies on the vertical axis for a random variable with two possible outcomes by using the equation below.

$$H = -x \log x - (1-x) \log(1-x) \quad (2.2)$$

H(X) versus P(x1) and P(x2)

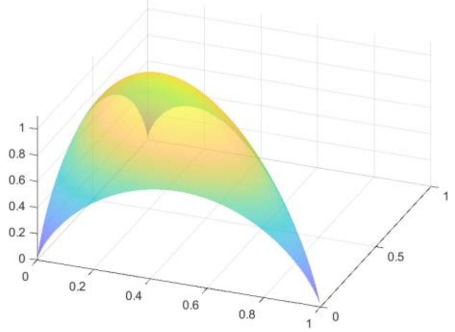


Fig. 2.2 Plots all possible Shannon entropies on the vertical axis for a random variable with two possible outcomes using the equation below. The graph was made partially see through to allow all the surface to be seen.

$$H = x \log x - y \log y - (1 - x - y) \log(1 - x - y) \quad (2.3)$$

The above graphs show all possible Shannon entropies for two and three random variables respectively. Below the graphs are the equations that specify the Shannon entropy plotted. There is no need to have a graph in three dimensions for the two-outcome system since there is an easily defined relation between both probabilities, and likewise for the three-outcome system. As can be seen there is a maximum where the probabilities of each event are equal. While these graphs show all possible values for the Shannon entropy of a system of two or three variables, one could calculate it for more random variables and find similar properties.

A more concrete example would be the roll of a six-sided die. Again, its entropy is greatest due to equal probabilities.

$$H(D6) = \sum {}^{1}/_{6} \log 6 = \log 6 = 0.778 \quad (2.4)$$

One could expand this to a 20-sided die in the shape of an icosahedron and find a similar result.

$$H(D20) = \log 20 = 1.301 \quad (2.5)$$

What this means is it would take one base ten digit to describe the six-sided die, and two base ten digits to describe the 20-sided die. One could expect this because of the number of sides each die has combined with the equal probabilities. Now if one were to change this to be in the context of a computer, base two would be far more effective.

$$H(D6) = \log_2 6 = 2.585 \quad (2.6)$$

$$H(D20) = \log_2 20 = 4.322 \quad (2.7)$$

From these examples in base two, it is clear we would need at least three bits to describe the six-sided die without any loss of information. We would also need five bits to describe the twenty-sided die. One could again predict this as the 2^3=8 is the smallest power of two greater than six and 2^5=32 is the smallest power of two greater than twenty.

Now if we changed the relative size of the sides such that one side had an 81% probability of being chosen and the rest had a 1% chance each, we would find very different results for the twenty-sided die.

$$H(Modified\ D20) = -0.19 \log 0.01 - 0.81 \log 0.81 = 0.454 \quad (2.8)$$

$$H(Modified\ D20) = -0.19 \log_2 0.01 - 0.81 \log_2 0.81 = 1.509 \quad (2.9)$$

This suggests we could somehow describe the die with as few as one base ten digit or two bits.

From these examples with dice we can also see the maximum value of Shannon entropy for any given system of N variables. It is only left to decide which base is best for the given scenario, such as base ten or binary.

$$H_{Max} = \log N \quad (2.10)$$

Why one would prefer to use Shannon entropy as opposed to the Heisenberg Uncertainty Principle or even the Robertson Uncertainty Principle should be growing clearer. The uncertainty principles thus far described will only tell you how precisely one can know two given observables at once. The Heisenberg Uncertainty only depending on the standard deviations of the observables and Robertson Uncertainty on the standard deviations and given state. These are both powerful tools but tell very little about the information content of a system and will not assist in testing the capabilities of a quantum key distribution method.

Shannon entropy also does not have the ability to provide one with the information needed, but from it a new analogous relation called the entropic uncertainty relation can be derived. This relation will characterize the entropy of a system allowing one to see a value analogous to classical information theory's Shannon entropy but evolved into the new Quantum Information world.

Chapter 3

Entropic Uncertainty Relation

The Entropic Uncertainty Relation for a qubit (or two-state quantum system) provides a lower bound on the sum of the Shannon entropies of two non-commuting observables of the qubit. The bound depends on the observables being considered, and how closely it is approached depends on the state of the qubit being considered. These points will be made clear by means of an example below. The work by Maassen and Uffink [4] provides the foundation for this section.

The Entropic Uncertainty Relation provides a lower bound for the sum of Shannon entropies of a quantum state and observables. This means that the amount of information stored in a quantum system has a lower bound that can be calculated. In the case of this relation the lower bound depends only on the maximum overlap of any two eigenstates in the observables under consideration, and hence it is independent of the given input state [1].

This entropic uncertainty relation is very powerful with regards to quantum key distribution. If one is to be sure they securely delivered the key, they will need to know about how much information is available to an eavesdropper. If the eavesdropper has access to enough information the encrypted message could be deciphered. The importance of the Entropic Uncertainty Relation rises when one needs to prove the security of their key distribution method. With the lower bound it provides it is possible to show that given protocol does will allow the eavesdropping attack to succeed [4].

With any tool it is important to understand how to use it. In this case a new interpretation of Shannon entropy is needed with regards to quantum mechanics. The answer is simply to use the eigenstates of the observable as the possible events and the probability of collapsing into any of these states as the probabilities. This gives us a value for the Shannon entropies of a quantum system.

$$H(X) = -\sum_i P(x_i)\log P(x_i) \quad (3.1)$$

$$P(x_i) = |\langle\psi|x_i\rangle|^2 \quad (3.2)$$

With the Shannon entropies of a quantum system defined, the lower bound of the uncertainty relation needs to be found. To find this, the maximum value for the probability of an eigenstate of one observable collapsing into the eigenstate of another observable upon measurement in the latter is needed. Expanding this method for multiple observables and higher-dimensional systems simply requires testing more pairs of eigenstates [1].

$$c = \max_{i,j} M_{i,j} = \max_{i,j}\left(\left|\langle x_i|z_j\rangle\right|^2\right) \quad (3.3)$$

Now that all the pieces necessary to construct the relation have been defined, one simply needs to put them together in such a way a lower bound is provided that does always work.

$$H(X) + H(Z) \geq \log {}^{1}\!/_{c} \quad (3.4)$$

In the case of qubits an important piece of information can be noticed to simplify parts of the analysis involved in the application of EUR. All possible values of c can be made to depend on one parameter inside the matrix $M_{i,j}$.

$$M_{i,j} = \begin{pmatrix} p & 1-p \\ 1-p & p \end{pmatrix} \quad (3.4)$$

Example

Qubit

Another example of the analysis of the Entropic Uncertainty Relation with regards to qubits is described by Durt [2].

The bases X and Z will be used in this example of the application of EUR. Basis X will be a copy of Z rotated counterclockwise by an angle α. Then there will be the input state $|\psi\rangle$ which will vary in its superposition.

$$|\psi\rangle = \cos {}^{\theta}/_{2}\, |+Z\rangle + \sin {}^{\theta}/_{2}\, |-Z\rangle \qquad (3.5)$$

To begin the Shannon entropy for Z is calculated

$$H(Z) = -\left(\cos {}^{\theta}/_{2}\right)^2 \log\left(\cos {}^{\theta}/_{2}\right)^2 - \left(\sin {}^{\theta}/_{2}\right)^2 \log\left(\sin {}^{\theta}/_{2}\right)^2 \quad (3.6)$$

Now we notice we can perform a transformation by rotating X by -α to get Z

$$H(X) = -\left(\cos\left[\frac{(\theta-\alpha)}{2}\right]\right)^2 \log\left(\cos\left[\frac{(\theta-\alpha)}{2}\right]\right)^2 - \left(\sin\left[\frac{(\theta-\alpha)}{2}\right]\right)^2 \log\left(\sin\left[\frac{(\theta-\alpha)}{2}\right]\right)^2 \quad (3.7)$$

Finally, the lower bound

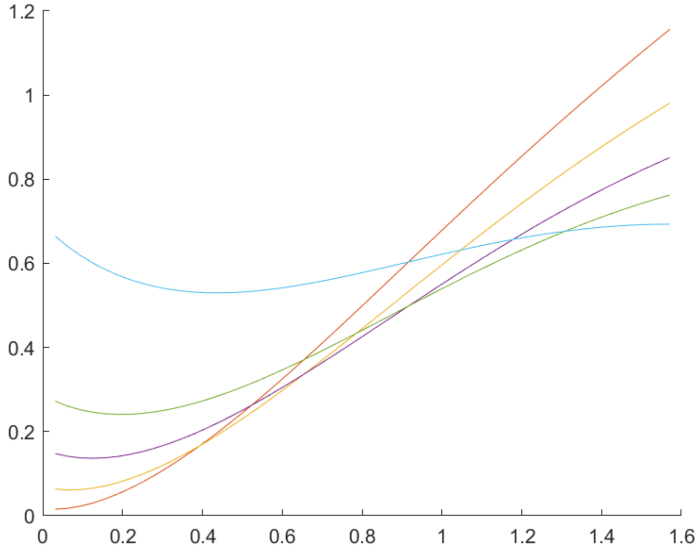
$$M_{i,j} = \begin{pmatrix} \cos^2 {}^{\alpha}/_{2} & \sin^2 {}^{\alpha}/_{2} \\ \sin^2 {}^{\alpha}/_{2} & \cos^2 {}^{\alpha}/_{2} \end{pmatrix} \qquad (3.8)$$

The maximum swaps when α = π/2

To demonstrate the effectiveness of the lower bound, it is subtracted from the Shannon entropy

$$H(X) + H(Z) - \log 1/c \quad (3.9)$$

Shannon entropy (H(X) +H(Z)) versus input state ψ



$$\alpha \ = {}^{\pi}/_{2}, {}^{\pi}/_{3}, {}^{\pi}/_{4}, {}^{\pi}/_{6}, {}^{\pi}/_{12}$$

Fig. 3.1 Shows all possible Shannon entropies H(X) +H(Z) for a qubit measured on two observables offset by angle α. The entropy values at 0 decrease as the offset decreases. It is interesting to note that with mutually unbiased bases the entropy varies very little, but as they get closer the entropy varies drastically with the input state.

$H(X) + H(Z) \ - \ \log 1/c$ versus input state ψ

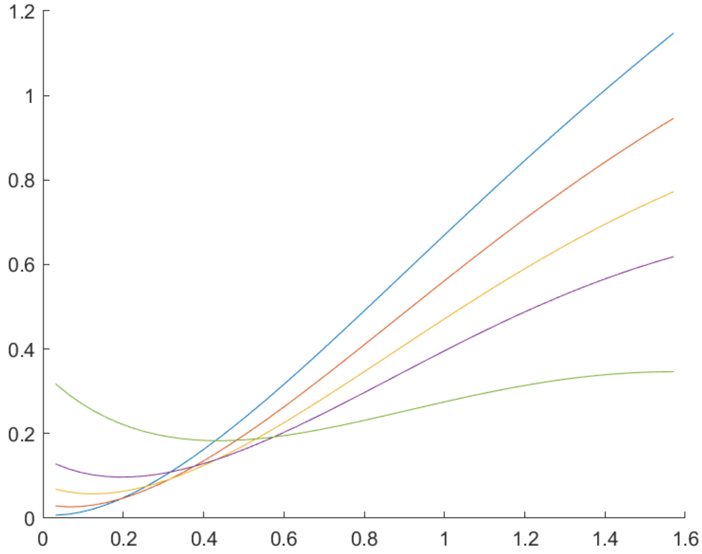


Fig. 3.2 demonstrates that the lower bound works as the curves never cross the ψ axis after the lower bound is subtracted

Qutrit

Further analysis of a qutrit system is provided by Rudnicki in his work [5].

A Qutrit is a quantum state with 3 dimensions. The math is similar and demonstrated below for state $|\psi\rangle$ with observables X and Z. Eigenstates without subscripts are in basis Z.

$$|\psi\rangle = \cos\alpha\,|0\rangle + \sin\alpha\cos\beta\,|1\rangle + \sin\alpha\sin\beta\,|2\rangle \text{ (3.10)}$$

$$|0\rangle_x = \frac{1}{\sqrt{2}}(-|0\rangle + |2\rangle) \text{ (3.11)}$$

$$|1\rangle_x = \frac{1}{2}\left(|0\rangle + \frac{1}{\sqrt{2}}|1\rangle + |2\rangle\right) \text{ (3.12)}$$

$$|2\rangle_x = \frac{1}{2}\left(|0\rangle - \frac{1}{\sqrt{2}}|1\rangle + |2\rangle\right) \text{ (3.13)}$$

Now P(X)

$$P(|0\rangle_x) = \frac{1}{2}(\cos\alpha + \sin\alpha\sin\beta)^2 \text{ (3.13)}$$

$$P(|1\rangle_x) = \frac{1}{4}\left(\cos\alpha + \sqrt{2}\sin\alpha\cos\beta + \sin\alpha\sin\beta\right)^2 \text{ (3.14)}$$

$$P(|2\rangle_x) = \frac{1}{4}\left(\cos\alpha - \sqrt{2}\sin\alpha\cos\beta + \sin\alpha\sin\beta\right)^2 \text{ (3.15)}$$

Then P(Z)

$$P(|0\rangle) = \cos^2\alpha \text{ (3.16)}$$

$$P(|1\rangle) = \sin^2\alpha\cos^2\beta \text{ (3.17)}$$

$$P(|2\rangle) = \sin^2\alpha\sin^2\beta \text{ (3.18)}$$

Finally, the lower bound

$$M_{i,j} = \begin{pmatrix} 1/2 & 1/4 & 1/4 \\ 0 & 1/2 & 1/2 \\ 1/2 & 1/4 & 1/4 \end{pmatrix} \text{ (3.19)}$$

Thus, the bound is $1/2$

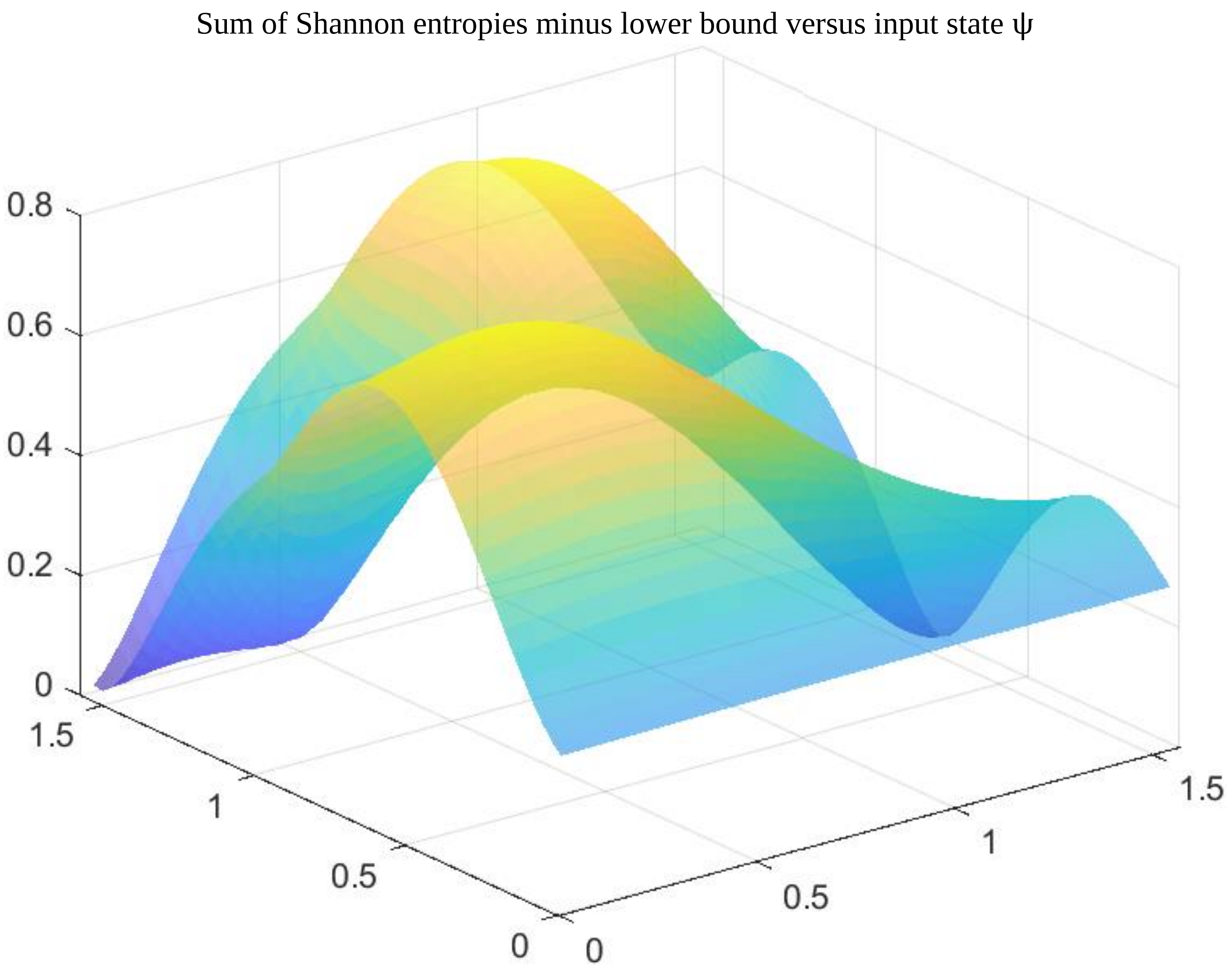


Fig. 3.3 plots all possible Shannon entropies for a qutrit and the given observables on the vertical axis and the two parameters defining the input state on the horizontal axis. The lower bound of ½ is subtracted to demonstrate that the EUR provides a lower bound to the relation. Where the surface approaches the horizontal plane, the inequality gets close to being saturated, whereas where it is high above that plane, there the uncertainties in both observables is large and one is far away from making the best possible measurements.

Conclusion

While the Heisenberg and Robertson uncertainty principles allow us to analyze the precision of measurements in quantum systems, they fail in certain applications where the measure they use (the standard deviation) does not capture the information needed for the application. This question is of far more consequence in quantum information theory. The problem of key distribution using quantum systems is one such application in which a different approach is needed.

The EURs, which use the Shannon entropy to quantify quantum information, meet the necessary requirements to investigate questions of security in quantum key distribution protocols.

This MQP has introduced the notion of Shannon information, EURs for qubits and qutrits and then illustrated them by means of simple calculations that show that the EURs are always satisfied. Further they also illustrate situations in which the EURs come close to being saturated (i.e. the equality is almost achieved).

The EURs studied here must be extended in at least three ways before they become relevant to the analysis of quantum key distribution protocols:

(1) They must be generalized to entangled quantum states shared by two parties, rather than just the states of a single party. This is of import as entanglement could be utilized by an eavesdropper to bypass any security one might have.
(2) They must be generalized to cover the measurements of three parties. Two of the parties are the ones exchanging the key, and the third is the eavesdropper.
(3) The notion of the Shannon entropy might have to be replaced by a more general measure known as the Renyi entropy in some cases, which would allow security protocols to be analyzed with the necessary degree of accuracy.

However, these goals go beyond the scope of this project and will have to be pursued elsewhere.

Bibliography

[1] Coles, Patrick J. et al. "Entropic Uncertainty Relations and Their Applications." Reviews of Modern Physics, vol. 89, no. 1, 2017, p. 015002, doi:10.1103/RevModPhys.89.015002.

[2] Durt, Thomas et al. "On Mutually Unbiased Bases." International Journal of Quantum Information, vol. 08, no. 04, 2010, pp. 535-640, doi:10.1142/S0219749910006502.

[3] Griffiths, David J. and Darrell F. Schroeter. Introduction to Quantum Mechanics. Third edition. ed., Cambridge University Press, 2018.

[4] Maassen, Hans and J. B. M. Uffink. "Generalized Entropic Uncertainty Relations." Physical Review Letters, vol. 60, no. 12, 1988, pp. 1103-06, doi:10.1103/PhysRevLett.60.1103.

[5] Rudnicki, Łukasz et al. "Strong Majorization Entropic Uncertainty Relations." Physical Review A, vol. 89, no. 5, 2014, p. 052115, doi:10.1103/PhysRevA.89.052115.

[6] Schumacher, Benjamin and Michael D. Westmoreland. Quantum Processes, Systems, and Information. Cambridge University Press, 2010.