Entropic uncertainty relations (EURs) and their connections to quantum key distribution protocols

by Ethan Washock

December 16, 2021

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 and *Mathematical Sciences*

Advisors

Professor P. K. Aravind

Professor Herman Servatius

Abstract

Quantum key distribution (QKD) protocols, processes which allow two parties to exchange a secret key by means of information encoded in qubits, are promising alternatives to classical cryptographic protocols. The security of these protocols can be analyzed using *entropic uncertainty relations* (EURs), which allow bounds to be placed on the amount of knowledge an eavesdropper can gain about the key by intercepting the qubits in transit. This report focuses on a generalization of the original EUR due to Maassen and Uffink by Berta et al. and explores its validity for several types of bipartite quantum states.

Acknowledgements

First, I'd like to thank the Mathematical Sciences student body here at WPI, from the undergraduates to the PhD students, for encouraging each other to think outside the box, consider outlandish problems and craft clever solutions. It has been a pleasure to know those that I have been able to meet personally and their view on mathematics has allowed me to grow over these past four years at WPI.

Second, I'd like to thank my family for their unconditional support—my parents, Karrie and Brian, and my brother Carter (a fellow WPI student currently, who will be working on his MQP in no time!).

Lastly, I'd like to thank my project advisor, Professor Aravind, for being a fantastic advisor whose feedback has been truly paramount. It has been an honor to know Professor from the time I was a freshman taking undergraduate classical mechanics to the later years when I took graduate quantum mechanics with him. I have not only learned a lot about physics from him, but I've also been thankful to learn some of the intricacies of academic writing from him while writing this report.

Contents

List of Figures

List of Tables

1 Introduction

Quantum computation, which uses two-state systems called qubits in place of classical computational bits to carry out calculations, is currently an area of great interest. One striking advantage of quantum computers was discovered by Peter Shor [13], who came up with an algorithm that could be executed on a quantum computer to factor large numbers in a much shorter time than the best classical computers. Shor's algorithm poses a problem for classical cryptographic protocols such as the RSA scheme of public key cryptography, whose security is derived from the fact that classical computers take an impractically long time to factor large numbers [6].

However, this threat to classical cryptography posed by quantum computers can be countered by using a new method for generating a secret key based on the exchange of qubits. The idea is for two parties to establish such a key by having one of them encode information in qubits that they send to the other. This secret key can then be used to encrypt and decrypt messages in the same fashion as in classical cryptography. If an eavesdropper attempts to measure the qubits while they are being sent to the intended receiver, they risk disturbing the qubits and causing errors in the private key. This disturbance can be detected by the parties and they can take steps to correct for it and generate a secure key.

The safety of quantum key generation is guaranteed by the fact that any observations on quantum systems generally cannot be made passively. Measuring a qubit in a random basis yields only partial information about it, and also leads, in the case of an incorrect measurement, to a disturbance of the original state that could reveal the presence of an eavesdropper. These limitations of measurements in quantum mechanics are captured mathematically through uncertainty relations such as those introduced by Heisenberg or Robertson. The issue with these relations is that they quantify uncertainty in terms of standard deviation, which isn't always a useful measure of our lack of knowledge about a physical quantity. A more useful measure, known simply as the *entropy*, was introduced by Claude Shannon in 1948 [12]. This notion of the Shannon entropy for a classical random variable was adapted to deal with the uncertainty of quantum states by von Neumann, after whom it is known as the *von Neumann entropy*.

Maassen and Uffink formulated a more general relation between the uncertainties of conjugate observables (such as the Pauli matrices `X` and `Z` for a system of two qubits) in 1988 [8], which used the conditional von Neumann entropy in place of the standard deviations used in Heisenberg's uncertainty principle. This was the first *entropic uncertainty relation* (abbreviated as EUR). It was modified by Berta et al. in 2010 [2] to account for the negative conditional entropy of a bipartite entangled state shared by two parties, since this is of interest in connection with quantum key exchange schemes. The Maassen-Uffink relation and its generalizations can be used to assess the security of various cryptographic protocols, and have been extensively studied for this reason. It is also for this reason that we study these relations in this project.

The first quantum key exchange protocol was devised by Charles Bennett and Gilles Brassard in 1984 [3]. It is known as the *BB84 protocol*, and is being actively used to this day. The protocol involves two

parties, Alice and Bob, with Alice encoding a secret key in a sequence of qubits and sending the qubits to Bob. Bob measures the qubits, communicates with Alice about his measurements, and the two are finally able to arrive at a secret key known only to them and no one else. A benefit of any quantum key exchange protocol is that an attempt by an eavesdropper to intercept and measure the qubits risks disturbing them and can be detected by the legitimate users. An entropic uncertainty relation for this protocol linking the uncertainties of Alice, Bob, and Eve can be formulated and is useful in estimating how much Eve knows about the key for the purposes of correcting for it.

We begin our report in Chapter 2 by discussing basic notions about qubits, systems of qubits, density matrices, and other topics from quantum mechanics necessary for understanding the later chapters of this report. Chapter 3 discusses the BB84 protocol and provides a basic analysis of its security. Chapter 4 introduces the Shannon entropy and its quantum-mechanical analogue, the von Neumann entropy. Chapter 5 discusses the Maassen-Uffink uncertainty relation along with its generalization due to Berta et. al [2]. The Berta et. al relation is important in connection with quantum key exchange protocols, so we discuss it in detail for a number of scenarios which illustrate the different ways in which degree of entanglement between the parties involved can affect the process. Lastly, Chapter 6 concludes with a brief recapitulation and discusses further topics that might have been studied but were not for lack of time.

2 Qubits and systems of qubits: basic ideas and notation

This section summarizes necessary material and notation from quantum mechanics that will be used throughout this report. We begin by discussing the definition of a qubit, and then showing how it can be extended to deal with the case of mixed states. We finish by discussing the use of tensor products to deal with systems of qubits.

2.1 What is a qubit?

Classical bits, the building block of modern computational systems, consist of zeroes and ones. The notion of a bit as a building block of computation can be extended to quantum mechanics with the introduction of a *qubit*.

A qubit is any two-state quantum system. A concrete example of a qubit is a spin-1/2 particle, such as an electron. A measurement of the spin along any direction can yield only two values, $+1$ or -1 (in units of $\hbar/2$). The z-component of spin for a qubit is represented by the Pauli matrix

$$\mathtt{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{1}$$

The eigenvectors of (1) with the eigenvalues $+1$ and -1 are

$$\begin{aligned} |0\rangle &\coloneqq \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ |1\rangle &\coloneqq \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{aligned} \tag{2}$$

The state $|0\rangle$ represents spin up (or eigenvalue $+1$) while $|1\rangle$ represents spin down (or eigenvalue -1) along the z-axis. The states $|0\rangle$ and $|1\rangle$ form an orthonormal basis for the two-dimensional Hilbert space of a qubit. The most general state of a qubit, referred to as a *pure state*, can be expressed as

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle,\ |\alpha|^2 + |\beta|^2 = 1 \tag{3}$$

By the Born rule, the probability that a qubit prepared in the state $|\psi\rangle$ will be found, upon measurement, to be in the state $|\phi\rangle$ is

$$\Pr(\phi|\psi) = |\langle\phi|\psi\rangle|^2 \tag{4}$$

The probability that (3) is found in the spin-up state is $\Pr(0|\psi)$ while the probability that it is found in the spin-down state is $\Pr(1|\psi)$. The sum of these probabilities is 1, which implies that

$$\Pr(0|\psi) + \Pr(1|\psi) = |\langle 0|\psi\rangle|^2 + |\langle 1|\psi\rangle|^2 = |\alpha|^2 + |\beta|^2 = 1 \tag{5}$$

(3) reveals one distinguishing feature of qubits: *superposition*. A classical bit can only be a 0 or a 1, while a qubit can be in a combination of both. More generally, the state of a qubit is a unit vector in $\mathbb{C}^2$ written in the form

$$|\Psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle,\ 0 \leq \theta \leq \pi,\ 0 \leq \phi \leq 2\pi \tag{6}$$

Replacing θ and ϕ in (6) with $\pi - \theta$ and $\pi - \phi$ allows us to construct the unit vector

$$|\Phi\rangle = \cos\left(\frac{\pi-\theta}{2}\right)|0\rangle + e^{i(\pi-\phi)}\sin\left(\frac{\theta+\pi}{2}\right)|1\rangle = \sin\frac{\theta}{2}|0\rangle - e^{-i\phi}\cos\frac{\theta}{2}|1\rangle \tag{7}$$

Computing the inner product of $|\Psi\rangle$ and $|\Phi\rangle$ yields 0, so $|\Psi\rangle$ and $|\Phi\rangle$ are orthogonal and form a two-dimensional basis in the Hilbert space of the qubit. These vectors correspond to the spin-up and spin-down states of the qubit along the direction characterized by the spherical angles θ and ϕ. As shown in Figure 1, the state (6) can be represented by the point with the spherical angles θ and ϕ on the surface of a unit sphere known as the *Bloch sphere*. Any antipodal pair of points on the surface of this sphere constitutes a basis, and one can see that there is an infinite choice of bases.

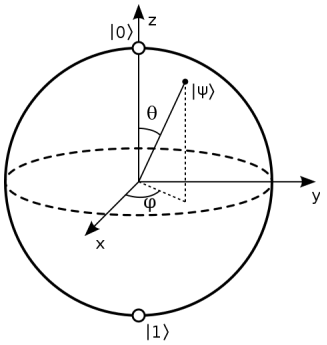

Figure 1: The *Bloch sphere*, which shows a geometric representation of the pure state space for a single qubit. Note that $|0\rangle$ and $|1\rangle$ are an orthonormal basis and are therefore diametrically opposite on the sphere (Smite-Meister (2009). Bloch sphere [photograph]. Wikimedia Commons. `https://upload.wikimedia.org/wikipedia/commons/thumb/6/6b/Bloch_sphere.svg/113px-Bloch_sphere.svg.png`)

The most commonly-used bases are the `X`, `Y`, and `Z` bases. These bases are named after the axis along which one measures the qubit's spin. Table 1 summarizes the important quantities connected with these

bases. `X`, `Y`, and `Z` are important in quantum cryptography, as we will see below, since they are *mutually unbiased bases*. Bases $\mathbb{X} = \{|x_1\rangle, \ldots, |x_n\rangle\}$ and $\mathbb{Y} = \{|y_1\rangle, \ldots, |y_n\rangle\}$ are mutually unbiased if

$$|\langle x_i|y_i\rangle|^2 = \frac{1}{n} \text{ for all } i, j \in \{1, \ldots, n\} \tag{8}$$

Each pair of the $\{\mathtt{X}, \mathtt{Y}, \mathtt{Z}\}$ bases are mutually unbiased. These bases are important due to the fact that if a particle is prepared in a spin up state along any one of these directions, then measuring it along one of the other two directions is equally likely to yield either spin up or down along that direction. This demonstrates that measuring in the incorrect basis yields no information about the state the particle was prepared in.

Basis	Pauli spin matrix	$+1$ eigenstate	-1 eigenstate
`X`	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\frac{1}{\sqrt{2}}(1,1)^\top = \|+\rangle$	$\frac{1}{\sqrt{2}}(1,-1)^\top = \|-\rangle$
`Y`	$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$	$\frac{1}{\sqrt{2}}(1,i)^\top = \|\uparrow\rangle$	$\frac{1}{\sqrt{2}}(1,-i)^\top = \|\downarrow\rangle$
`Z`	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	$(1,0)^\top = \|0\rangle$	$(0,1)^\top = \|1\rangle$

Table 1: Commonly-used bases in quantum information theory, along with the notation that will be used for their eigenstates in this report.

2.2 Mixed states and density matrices

The most general state of a qubit is not a pure state but a mixed state.

Definition. *A **mixed state** is a set $\{|\psi_1\rangle, \ldots, |\psi_k\rangle\}$ of pure states (unit vectors) in $\mathbb{C}^d$ together with a set of probabilities $\{p_1, \ldots, p_k\}$ summing to 1 such that the state $|\psi_k\rangle$ is prepared with the probability p_k. A pure state is a special case of a mixed state in which $k = 1$.*

Mixed states can arise in two different ways. Firstly, mixed states can arise if one is unsure of how the state was prepared. Secondly, mixed states can arise if one looks at only a few qubits of a composite system consisting of a larger number of qubits (for example, if one has a system of two qubits, looks at just one of these qubits, and ignores the other, its state would be a mixed state). Mixed states are common in quantum cryptography, since the qubit interacts with its environment and other qubits. The mixed state defined above can be represented by the **density matrix**

$$\rho = \sum_{i=1}^{k} p_i |\psi_i\rangle\langle\psi_i| \tag{9}$$

One can diagonalize this density matrix to determine its eigenvalues and eigenvectors. Its eigenvalues are a set of positive numbers (some of which could be 0) summing to 1, while the corresponding eigenvectors are an orthogonal set of vectors in $\mathbb{C}^d$. This set of eigenvalues and eigenvectors allows the density matrix to be interpreted as the mixed state consisting of a set of mutually orthogonal pure states (the eigenvectors), with each occurring with a probability given by the corresponding eigenvalue. Since the trace of the density matrix is the sum of its eigenvalues, and the eigenvalues sum to 1, it follows that

$$\mathrm{Tr}(\rho) = 1 \tag{10}$$

Example 1. A qubit which can be in the state $|0\rangle$ with probability $p \in [0, 1]$ or in the state $|1\rangle$ with probability $1 - p$ has the density matrix

$$\rho_1 = p|0\rangle\langle 0| + (1-p)|1\rangle\langle 1| = \begin{pmatrix} p & 0 \\ 0 & 1-p \end{pmatrix} \tag{11}$$

More generally, the matrix

$$\rho_2 = p|\psi\rangle\langle\psi| + (1-p)|\psi^\perp\rangle\langle\psi^\perp| \tag{12}$$

is a density matrix for any value $p \in [0, 1]$ and any two orthogonal unit vectors in $\mathbb{C}^2$ denoted $|\psi\rangle$ and $|\psi^\perp\rangle$. Since $\rho_2|\psi\rangle = p|\psi\rangle$ and $\rho_2|\psi^\perp\rangle = (1-p)|\psi^\perp\rangle$, ρ_2 has eigenvalues of p and $1 - p$. Summing the eigenvalues of ρ_2 shows that (10) is satisfied.

One can calculate the expectation values of observables using density matrices, similar to the calculations for standard kets. For an observable A and a density matrix ρ, the expectation value of A in the state described by ρ is equal to

$$\langle A\rangle = \mathrm{Tr}(\rho A) \tag{13}$$

Example 2. Let ρ_1 be the density matrix from Example 1. Let $A = \mathtt{X} + \mathtt{Z}$. A is Hermitian, and therefore a valid observable. By routine calculation,

$$\rho_1 A = \begin{pmatrix} p & 0 \\ 0 & 1-p \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} p & p \\ 1-p & p-1 \end{pmatrix} \tag{14}$$

It follows from (14) that $\langle A\rangle = \mathrm{Tr}(\rho_1 A) = 2p - 1$.

2.3 Tensor products and entanglement

Two systems whose states exist in separate Hilbert spaces can be described in a larger Hilbert space that is called the *tensor product* of the spaces.

Definition. *Let $\mathcal{H}_A, \mathcal{H}_B$ be two Hilbert spaces. The tensor product of $\mathcal{H}_A$ and $\mathcal{H}_B$, denoted $\mathcal{H}_A \otimes \mathcal{H}_B$, is defined by the following properties:*

1. ***Closure under tensor products:*** *For all $|a\rangle$ in $\mathcal{H}_A$ and all $|b\rangle$ in $\mathcal{H}_B$, $|a\rangle \otimes |b\rangle$ is in $\mathcal{H}_A \otimes \mathcal{H}_B$. We denote $|a\rangle \otimes |b\rangle \coloneqq |ab\rangle$.*

2. ***Linearity:*** *For $|b_1\rangle, |b_2\rangle$ in $\mathcal{H}_B$, c_1 and c_2 in $\mathbb{C}$, and $|a\rangle \in \mathcal{H}_A$,*

$$|a\rangle \otimes (c_1 |b_1\rangle + c_2 |b_2\rangle) = c_1 (|a\rangle \otimes |b_1\rangle) + c_2 (|a\rangle \otimes |b_2\rangle) \tag{15}$$

   Linearity also holds for linear combinations of vectors in $\mathcal{H}_A$.

3. ***Adjoints:*** *For $|ab\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$, its adjoint, denoted $\langle ab|$, is in $\mathcal{H}_A \otimes \mathcal{H}_B$.*

4. ***Inner products:*** *For $|a_1 b_1\rangle, |a_2 b_2\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$,*

$$\langle a_1 b_1 | a_2 b_2 \rangle = \langle a_1 | b_1 \rangle \langle a_2 | b_2 \rangle \tag{16}$$

5. ***Closure under superpositions:*** *$\mathcal{H}_A \otimes \mathcal{H}_B$ is closed under linear combinations of vectors.*

Since the tensor product of two Hilbert spaces is closed under linear combinations of vectors, the tensor product of the spaces is a vector space as well. The vector space of systems of two qubits is a 4-dimensional Hilbert space spanned by the vectors $\{|ij\rangle\}_{0 \leq i,j \leq 1}$. The most general pure state of a two-qubit system can be written as

$$|\Psi_{AB}\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle, \ \alpha_{00}, \alpha_{01}, \alpha_{10}, \alpha_{11} \in \mathbb{C} \tag{17}$$

$$|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1 \tag{18}$$

It is possible that a state living in the space $\mathbb{C}^2 \otimes \mathbb{C}^2$ is not the tensor product of two states in $\mathbb{C}^2$. For $a_0, a_1, b_0, b_1 \in \mathbb{C}$, it is easy to see that

$$(a_0|0\rangle + a_1|1\rangle) \otimes (b_0|0\rangle + b_1|1\rangle) = a_0 b_0|00\rangle + a_0 b_1|01\rangle + a_1 b_0|10\rangle + a_1 b_1|11\rangle \tag{19}$$

It follows from (19) that $|\psi_{AB}\rangle = c_{00}|00\rangle + c_{01}|01\rangle + c_{10}|10\rangle + c_{11}|11\rangle$ can be written as a tensor product if and only if

$$c_{00}c_{11} = c_{01}c_{10} \tag{20}$$

If a state in $\mathbb{C}^2 \otimes \mathbb{C}^2$ doesn't satisfy (20), it cannot be represented as a tensor product of two states and is said to be an entangled state.

Definition. *A state $|\psi\rangle$ is **entangled** if it cannot be represented as the tensor product of two vectors. Any state which can be represented as the tensor product of two states (and therefore not entangled) is called a **product state**.*

Example 3. The state $|\psi\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$ is a product state, since it can be written as $(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle) \otimes (\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle)$.

Example 4. Let $|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle$ and $|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$. By (20), the states $|\Phi^{\pm}\rangle$ and $|\Psi^{\pm}\rangle$ are entangled. These two-qubit states are referred to as the **Bell states**.

Entangled states have many counterintuitive properties. For example, if two qubits in an entangled state are at distant locations, their properties can be correlated in surprising ways that defy simple explanation. These surprising features are fully explained in Bell's theorem, and they are also important in many practical applications such as the transmission of quantum information by teleportation [1]. For example, one intriguing property of an entangled state can be seen by writing the Bell state $|\Phi^+\rangle$ in the `X` basis for both qubits:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}\left(\left(\frac{|+\rangle + |-\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|+\rangle + |-\rangle}{\sqrt{2}}\right) + \left(\frac{|+\rangle - |-\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|+\rangle - |-\rangle}{\sqrt{2}}\right)\right). \tag{21}$$

Using the linearity property of the tensor product, equation (21) can be simplified to

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|++\rangle + |--\rangle) \tag{22}$$

(22) shows that not only do the measurements of qubits A and B match when both are measured in the `Z` basis, but also when they are measured in the `X` basis.

3 Secure communications in the quantum realm

This section discusses the motivation for quantum cryptographic protocols and the first protocol of this kind proposed by Bennett and Brassard in 1984, now known simply as BB84 [3]. Among the good general introductions to this topic are books by Schumacher [11], Nielsen and Chuang [9], and Wootters [7].

3.1 The motivation behind quantum protocols

Assume that Alice wants to send a binary message of length n to Bob. We denote this message the *plaintext*. Alice creates a binary string of length n called the *key* to encrypt this message. The plaintext and the key are vectors in the vector space $\mathbb{Z}_2^n$, denoted P and K respectively. Alice can encrypt the plaintext by computing $P + K$. The resultant string of encrypted bits, called the *ciphertext* (denoted C), can be sent to Bob. Once Alice has sent the key to Bob, Bob can convert the ciphertext back to the plaintext by computing

$$C + K = (P + K) + K = P + 2K = P \tag{23}$$

The problem with this procedure is that the secret key used by Alice to encrypt the message and by Bob to decrypt it must be shared between them in some way without anyone else learning about it. The BB84 protocol allows Alice to send the key to Bob while ensuring that no knowledge about it falls into the hands of a third party.

3.2 The BB84 Protocol

The BB84 protocol consists of the following steps:

Step 1: Alice sends the key in a sequence of qubits.

Alice begins by generating two random binary strings of length k. These are referred to as the "basis string" and the "parent string" , with the parent string being a long random string of 0's and 1's out of which the secret key shared by Alice and Bob will be distilled. Alice prepares a system of qubits using the two strings. The basis string denotes the basis in which Alice encodes each qubit (`Z` for 0, or `X` for 1). The parent string denotes the eigenvalue of each qubit for the chosen basis (+1 for 0, −1 for 1). See Table 2 for full details of how Alice prepares each qubit when given a combination of values in the basis and parent strings.

Parent string value	0	0	1	1
Basis string value	0	1	0	1
Corresponding qubit state	$\|0\rangle$	$\|+\rangle$	$\|1\rangle$	$\|-\rangle$

Table 2: How Alice uses each component of the parent and basis string to prepare each qubit sent to Bob.

Step 2: Bob measures Alice's qubits using his own version of the basis string.

The system of qubits prepared by Alice is transmitted to Bob. Bob doesn't know which basis Alice prepared each qubit in, so he generates a random string of 0's and 1's of the same length as the received string, which serves as his own version of the basis string. Bob uses his version of the basis string to measure each qubit he gets from Alice.

Step 3: Alice announces her basis string.

Alice tells Bob through a public channel the basis that she prepared each of her qubits in without disclosing the eigenvalue of each qubit. Bob then tells Alice which of his bases matched hers. If Bob's measurement basis disagrees with Alice's for a certain qubit, the corresponding bit is discarded. The remaining qubits were measured in the correct basis, so the corresponding entries of the parent string, which are known to both Alice and Bob, can be kept by them as the "raw" key from which their final key can be distilled.

Step 4: Alice and Bob check a selection of bits in the key for errors.

Note that the secret key obtained by Alice and Bob in Step 3 need not be perfect. Some of the qubits might have been subjected to noise in the quantum channel when Alice transmitted them to Bob, or the system may have been disturbed by the interference of an eavesdropper. To identity and mitigate errors, Alice and Bob compare a selection of their key to see whether Bob's key matches Alice's transmitted key. The error rate in this sample is assumed to be the same as in the rest of the key. They discard the portion of the key they compared, since it is not secret any more.

Step 5: Bob applies classical cryptography techniques to recover the rest of the message.

If the error rate in the raw key found by Alice and Bob at the end of Step 4 is less than a certain critical amount, then Alice and Bob can use two techniques of classical cryptography known as *information reconciliation and privacy amplification* to distill a secret key from it. These two processes shrink their raw key further until there is virtually no discrepancy in the bits shared by Alice and Bob and any information that an eavesdropper might have had about the bits in the raw key has been reduced to zero.

Alice's basis string	0	0	1	0	0	1	1	1
Alice's parent string	0	1	0	1	0	1	1	0
Alice's system of qubits	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|1\rangle$	$\|0\rangle$	$\|-\rangle$	$\|-\rangle$	$\|+\rangle$
Bob's basis string	0	1	0	0	1	1	0	1
Bob's measurement	$\|0\rangle$	$\|+\rangle$	$\|0\rangle$	$\|1\rangle$	$\|-\rangle$	$\|-\rangle$	$\|0\rangle$	$\|+\rangle$
Bob's parent string	0	0	0	1	1	1	0	0
Do their bases match?	YES	NO	NO	YES	NO	YES	NO	YES
Their shared key	0			1		1		0

Table 3: An example of the BB84 protocol in action.

3.3 The security of BB84: elementary considerations

The BB84 protocol is designed to ensure that the two corrective measures noted in Step 5 can be implemented successfully. The details of how this can be done are complicated, but in the rest of this section we discuss some elementary aspects of this procedure.

Let us point out first a simple way in which an eavesdropper's presence can be detected. Assume that an eavesdropper, Eve, mistakenly measured a qubit in the `Z` basis when it was originally prepared in the `X` basis. Eve prepares an eigenstate of `Z` in place of Alice's original qubit and then sends it on to Bob. Bob measures the qubit he gets from Eve in the `X` basis but could discover that the corresponding bit in Alice's key disagrees with his key during his later public exchange with Alice.

Let us calculate the probability that Alice and Bob can detect Eve's interference by checking n bits of their shared key. The probability that Eve measures a qubit in the wrong basis is $1/2$, but the probability that Bob then infers the wrong bit later is $1/2$. Thus, the probability of Eve's interference being detected is $(1/2)\cdot(1/2) = 1/4$. Eve's probability of learning Alice's bit correctly without being detected is therefore $3/4$. If Alice and Bob compare n bits of their shared key, the probabilty of them noticing at least one error is $1 - (3/4)^n$, which becomes arbitrarily close to 1 as n becomes large. By checking just 100 bits, for example, they can tell within a tiny fraction of a percent whether there has been interference or not, either from an eavesdropper or as a result of channel noise.

The reason Alice transmits in the `Z` and `X` bases is that this minimizes the amount of knowledge that can be gleaned by Eve. To see this more clearly, suppose that Alice uses the orthonormal bases `Z` and $\mathtt{U}_\theta$ for a parameter $\theta \in [0, \pi/2]$. The basis $\mathtt{U}_\theta$ is the basis `Z` rotated by an angle of θ from the z-axis. So, if the $+1$ and -1 eigenvectors of $\mathtt{U}_\theta$ are denoted $|u^{(+)}\rangle$ and $|u^{(-)}\rangle$ respectively,

$$\left|\left\langle u^{(+)}|0\right\rangle\right|^2 = \left|\left\langle u^{(-)}|1\right\rangle\right|^2 = \cos^2\frac{\theta}{2} \tag{24}$$

$$\left|\left\langle u^{(+)}|1\right\rangle\right|^2 = \left|\left\langle u^{(-)}|0\right\rangle\right|^2 = \sin^2\frac{\theta}{2} \tag{25}$$

Let's say that Eve intercepts the message. She measures each of the qubits randomly in either Z or U_θ and then transmits the state she gets to Bob. One can compute the probability, P_E, that Eve correctly deciphers the information in a typical qubit sent by Alice. We will not consider the cases in which Alice and Bob measure in different bases, since these bits end up getting discarded. If Eve measures the qubit in the correct basis, the probability of an accurate measurement is 1. However, if Alice prepares in the `Z` basis and Eve measures in the $\mathtt{U}_\theta$ basis, the probability that Eve's measurement matches Alice's bit is

$$\begin{aligned} P_E &= \Pr\left(u^{(+)} \mid 0\right)\Pr(0) + \Pr\left(u^{(-)} \mid 1\right)\Pr(1) \\ &= \frac{1}{2}\left|\left\langle u^{(+)} \mid 0\right\rangle\right|^2 + \frac{1}{2}\left|\left\langle u^{(-)} \mid 1\right\rangle\right|^2 \\ &= \frac{1}{2}\cos^2\frac{\theta}{2} + \frac{1}{2}\cos^2\frac{\theta}{2} \\ &= \cos^2\frac{\theta}{2} \end{aligned} \tag{26}$$

Similarly, if Alice prepares in the $\mathtt{U}_\theta$ basis and Eve measures in the `Z` basis; the probability that Eve's measurement matches Alice's parent string is

$$\begin{aligned} P_E &= \Pr\left(0 \mid u^{(+)}\right)\Pr(u^{(+)}) + \Pr\left(1 \mid u^{(-)}\right)\Pr(u^{(-)}) \\ &= \frac{1}{2}\left|\left\langle 0 \mid u^{(+)}\right\rangle\right|^2 + \frac{1}{2}\left|\left\langle 1 \mid u^{(-)}\right\rangle\right|^2 \\ &= \cos^2\frac{\theta}{2} \end{aligned} \tag{27}$$

Since the probabilities of Alice and Eve choosing their bases are independent, the probability that Eve gets the correct measurement when measuring a qubit is the average of P_E over each basis choice for Alice and Eve:

$$P_{E,success} = \frac{1}{4}\left(1 + 1 + \cos^2\frac{\theta}{2} + \cos^2\frac{\theta}{2}\right) = \frac{1}{2}\left(1 + \cos^2\frac{\theta}{2}\right) = \frac{3 + \cos\theta}{4} \tag{28}$$

$P_{E,success}$ is maximized when $\theta = 0$, corresponding to the basis $\mathtt{U}_0 = \{|0\rangle, |1\rangle\} = \mathtt{Z}$. On the other hand, $P_{E,success}$ is minimized when $\theta = \pi/2$, which gives a value of $P_{E,success} = 3/4$. A basis that is an angle of $\pi/2$ radians from the `Z` basis is `X`. This means that *using the X and Z bases minimize the probability that Eve measures each qubit correctly.* The use of mutually unbiased bases, like `Z` and `X`, is common in cryptographic protocols because it allows an eavesdropper who measures a qubit in the wrong basis to get no information about the bit transmitted through it.

4 Quantifying uncertainty – uncertainty principles and entropy

In this section, we discuss the classical uncertainty relations in quantum mechanics and point out their drawbacks in relation to information theory. We discuss how the Shannon entropy can be used as a better measure of uncertainty and then discuss how the von Neumann entropy can be introduced to capture the uncertainty present in the state of a system of qubits.

4.1 Classical uncertainty relations in quantum measurements

Uncertainty is at the heart of quantum mechanics. The first statement regarding the relationship between the uncertainties of two noncommuting observables was made by Werner Heisenberg in 1927. The expectation value of an observable A for the state $|\psi\rangle$ is defined to be

$$E[A] \coloneqq \langle\psi|A|\psi\rangle = \langle A\rangle \tag{29}$$

The uncertainty associated with an observable A, denoted ΔA, is defined to be

$$\Delta A = \sqrt{\langle A^2\rangle - \langle A\rangle^2} \tag{30}$$

Heisenberg observed in his **Heisenberg uncertainty principle** that

$$\Delta\hat{x}\Delta\hat{p} \geq \frac{\hbar}{2} \tag{31}$$

where $\hat{x}$ and $\hat{p}$ are the particle's position and momentum, respectively. This principle reveals that a higher accuracy of measurement for one observable results in a lower accuracy of measurement for the other observable. Since $\Delta\hat{p} \geq \hbar/(2\Delta\hat{x})$, even if the bound is saturated (the bound is met with equality), decreasing $\Delta\hat{x}$ means that $\Delta\hat{p}$ must increase.

A more general relationship between the uncertainties of two noncommuting observables was made by Howard Robertson in 1929. The commutator of two $n \times n$ matrices A and B is defined to be

$$[A, B] \coloneqq AB - BA \tag{32}$$

Robertson stated in his **Robertson uncertainty principle** that for two noncommuting observables A and B,

$$\Delta A \Delta B \geq \frac{1}{2}|\langle [A,B] \rangle| = \frac{1}{2}|\langle \psi | [A,B] | \psi \rangle| \tag{33}$$

It is worth noting that the lower bound on the right of (33) depends upon the state in which the expectation value of the commutator $[A, B]$ is evaluated. This contrasts with (31), in which the lower bound is absolute.

Example 5. $[\hat{x}, \hat{p}] = i\hbar I$, so $\hat{x}$ and $\hat{p}$ are noncommuting observables. Substituting $[\hat{x}, \hat{p}] = i\hbar I$ into (33) yields

$$\Delta \hat{x} \Delta \hat{p} \geq \frac{1}{2}|\langle [\hat{x}, \hat{p}] \rangle| = \frac{1}{2}|\langle i\hbar I \rangle| = \frac{\hbar}{2} \tag{34}$$

This results in Heisenberg's uncertainty principle (eq. (31)).

4.2 Uncertainty of classical information

The aforementioned measures of uncertainty don't adequately capture our lack of knowledge about the state of a system. For example, there may be a 10 percent chance that it rains on Monday, a 20 percent chance that it rains on Tuesday, and a 40 percent chance that it rains on Wednesday. The standard deviation of the percentage about its average value is not a terribly useful measure of our state of uncertainty about the weather throughout the course of the week. There is also no way to calculate how much information one knows about a measurement given the result of a prior measurement. A better measure of uncertainty for a probability distribution is the *entropy*, a concept first introduced by Claude Shannon in 1948 [12] (henceforth, the term entropy without qualification will always mean the Shannon entropy and not the thermodynamic entropy).

Definition. *Let X be a random variable with finitely many outcomes. The* ***entropy*** *of the distribution X is equal to*

$$H(X) = -\sum_{x \in X} \Pr(x) \log_2(\Pr(x)) \tag{35}$$

where $\Pr(x)$ *is the probability that the variable X has the outcome x.*

The use of the base-2 logarithm in this definition implies that the entropy is measured in bits. We will measure entropy and information in bits throughout this report. The entropy of a random variable has a simple meaning: it can be thought of as the average number of yes/no questions that must be asked to determine the outcome of that variable.

Example 6. A coin has possibilities of heads (H) and tails (T) with probabilities $\Pr(\mathrm{H}) = p$ and $\Pr(\mathrm{T}) = 1 - p$ for some $p \in [0, 1]$. The entropy of the distribution as a function of p equals

$$H(p) = -p\log_2(p) - (1-p)\log_2(1-p),\ p \in [0,1] \tag{36}$$

This is referred to as the **binary entropy function**. A few properties of this function are:

- The minimum of the function is achieved at $p = 0$ and $p = 1$ (when only one of the two events can occur), and then $H(0) = H(1) = 0$.
- The maximum of the function is achieved at $p = 1/2$ (when both events occur with equal probability), and then $H(1/2) = 1$.
- $H(p) \geq 0$ for all $p \in [0,1]$.

The entropy is also known as the *surprisal*. When the entropy is small, we know with a greater certainty what the result of the measurement will be. Surprisal is minimized for the entropy function in (36) at $p = 0$ and $p = 1$, which makes sense considering that only one result can occur in each of these cases. The surprisal is highest when both outcomes are equally likely to occur (which corresponds to a uniform distribution).

Another type of uncertainty that we are interested in is the uncertainty of a random variable given the knowledge of another random variable. The joint entropy can be calculated for any pair of random variables as follows:

Definition. *Let X, Y be a pair of random variables with finitely many outcomes. For $x \in X$ and $y \in Y$, let $\Pr(x,y)$ denote the probability of both x and y occurring. The **joint entropy** of X and Y, denoted $H(X,Y)$, is equal to*

$$H(X,Y) = -\sum_{x\in X}\sum_{y\in Y}\Pr(x,y)\log_2(\Pr(x,y)) \tag{37}$$

The joint entropy can be used to calculate the conditional entropy of either of the two random variables.

Definition. *Let X, Y be a pair of random variables with finitely many outcomes. The **entropy of** X **conditional on knowing** Y, denoted $H(X|Y)$, is equal to*

$$H(X|Y) = H(X,Y) - H(Y) \tag{38}$$

This conditional entropy characterizes the uncertainty of one variable when given information about another variable. Note that if one is given only the set of probabilities $\{\Pr(x,y) : x \in X,\, y \in Y\}$ for a set of discrete random variables X and Y, $H(Y)$ can be calculated by noting that for any $y \in Y$,

$$\Pr(y) = \sum_{x\in X}\Pr(x,y) \tag{39}$$

It follows from this definition that given a set of discrete random variables X and Y along with a set of probabilities $\{\Pr(x, y) : x \in X,\, y \in Y\}$,

$$H(Y) = -\sum_{y \in Y} \Pr(y_i) \log_2 \Pr(y_i) \tag{40}$$

Useful properties of the entropy function are listed in Table 4.

Non-negativity	$H(X) \geq 0$
Bounding value	$H(X) \leq \log_2(\lvert X \rvert)$
Maximal entropy	$H(X) = \log_2(\lvert X \rvert)$ if and only if X is a uniform distribution
Bounding conditional entropy	$H(X\lvert Y) \leq H(X)$
Maximal conditional entropy	$H(X\lvert Y) = H(X)$ if X and Y are independent.

Table 4: Properties of the entropy function for discrete random variables X, Y [5].

Example 7. Let X, Y be two random variables each having possible values $\{0, 1\}$. For a value $p \in [0, 1]$, assume that

$$\Pr(0, 1) = \Pr(1, 0) = 0,\ \Pr(0, 0) = p,\ \Pr(1, 1) = 1 - p \tag{41}$$

where $\Pr(\mathtt{a}, \mathtt{b})$ denotes the probability that $\mathtt{a}$ is a result of X and $\mathtt{b}$ is the result of Y. By (37),

$$H(X, Y) = -p \log_2(p) - (1 - p) \log_2(1 - p) \tag{42}$$

Applying (35) and (39) to the random variable X gives

$$H(X) = -p \log_2(p) - (1 - p) \log_2(1 - p) \tag{43}$$

It follows by (38) that

$$H(Y|X) = H(X, Y) - H(X) = 0 \tag{44}$$

This shows that no matter the choice of p, the result of Y is known with certainty when the result of X is known. This makes sense, considering that regardless of the p value, one knows that the value of X and Y match with 100 percent certainty.

Two random variables which are completely uncorrelated from one another are called *independent*.

Definition. *Let X and Y be two discrete random variables with finitely many outcomes. X and Y are* ***independent*** *if for all $x \in X$ and $y \in Y$, $\Pr(x, y) = \Pr(x)\Pr(y)$.*

An example of independent random variables can be seen by flipping a coin. One flip of a coin has no impact on the result of the next flip, so the result of the first coin flip is independent of the result of the second coin flip for a fair coin. Knowing that two random variables X and Y are independent allows (37) to simplify down to

$$\begin{aligned} H(X,Y) &= \sum_{x\in X}\sum_{y\in Y} \Pr(x)\Pr(y)\left(\log_2(\Pr(x)) + \log_2(\Pr(y))\right) \\ &= -\sum_{x\in X}\Pr(x)\log_2(\Pr(x))\sum_{y\in Y}\Pr(y) - \sum_{y\in Y}\Pr(y)\log_2(\Pr(y))\sum_{x\in X}\Pr(x) \\ &= -\sum_{x\in X}\Pr(x)\log_2(\Pr(x)) - \sum_{y\in Y}\Pr(y)\log_2(\Pr(y)) \\ &= H(X) + H(Y) \end{aligned} \tag{45}$$

By equations (38) and (45), for independent, discrete random variables X and Y, $H(X|Y) = H(X) + H(Y) - H(Y) = H(X)$. This signifies that the knowledge of the result of Y does nothing to improve our knowledge of the result of X.

4.3 Uncertainty of quantum information

The calculation of entropies for a density matrix is very similar to the calculations for a classical probability distribution. The eigenvalues of a density matrix specify the probabilities of the pure states in it, and its entropy can be calculated in the manner explained below.

Definition. *Let ρ be the density matrix of a quantum state with eigenvalues $\{\lambda_1, \ldots, \lambda_n\}$. The* ***von Neumann entropy*** *of the state ρ is equal to*

$$H(\rho) = -\sum_{j=1}^{n} \lambda_j \log_2(\lambda_j) \tag{46}$$

We define $0 \cdot \log_2 0 \coloneqq 0$, so events with probability zero do not contribute to the entropy. The von Neumann entropy of a pure state is zero, but that of a mixed state is always positive.

Example 8. Consider the density matrix of a mixed state consisting of the pure states $|00\rangle$ and $|11\rangle$, with probabilities $\cos^2\frac{\theta}{2}$ and $\sin^2\frac{\theta}{2}$, respectively, for $\theta \in [0, \pi/2]$. Then,

$$\rho = \cos^2\frac{\theta}{2}|00\rangle\langle 00| + \sin^2\frac{\theta}{2}|11\rangle\langle 11| \tag{47}$$

Denoting the set of eigenvalues of the matrix A by $\mathtt{ev}(A)$, one finds that $\mathtt{ev}(\rho) = \{\cos^2\theta, 0, 0, \sin^2\theta\}$, so

$$H(\rho) = -\cos^2\frac{\theta}{2}\log_2\cos^2\frac{\theta}{2} - \sin^2\frac{\theta}{2}\log_2\sin^2\frac{\theta}{2} \tag{48}$$

Consider the density matrix of a bipartite system, which consists of two qubits. However, each qubit may be in the possession of a different observer, with one holding the first and the other the second. Each observer will observe his (or her) qubit to be in a mixed state whose density matrix can be calculated as indicated below.

Definition. *Let $\rho_{AB} = \sum_{j,j'=0}^{1}\sum_{k,k'=0}^{1} c_{jk,j'k'}|jk\rangle\langle j'k'|$, where $c_{jk,j'k'} \in \mathbb{C}$ for $j,k,j',k' \in \{0,1\}$, be the density matrix of a two-qubit system consisting of the separate qubits A and B. We define the* ***partial trace over B*** *of ρ_{AB}, denoted $\rho_A = \mathrm{Tr}_B\,\rho_{AB}$, to be*

$$\rho_A = \sum_{k=0}^{1}\sum_{j,j'=0}^{1} c_{jk,j'k}|j\rangle\langle j'| \tag{49}$$

Similarly, we define the ***partial trace over A*** *of ρ_{AB}, denoted $\rho_B = \mathrm{Tr}_A\,\rho_{AB}$, to be*

$$\rho_B = \sum_{j=0}^{1}\sum_{k,k'=0}^{1} c_{jk,jk'}|k\rangle\langle k'| \tag{50}$$

ρ_A and ρ_B represent the so-called ***reduced density matrices*** *of qubit A or B when each is considered by itself.*

The entropy of the matrices ρ_A and ρ_B can be calculated in terms of their eigenvalues using (46).

Example 9. Let $\rho_{AB} = \frac{1}{2}|00\rangle\langle 00| + \frac{1}{2}|10\rangle\langle 10|$ be the density matrix of a two-qubit system. If the second qubit, B, is measured in the z-direction, it will be found in the state $|0\rangle$ with absolute certainty. Therefore, we should expect the entropy of the reduced density matrix ρ_B to be zero. Calculating the reduced density matrix ρ_B gives

$$\rho_B = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \tag{51}$$

The eigenvalues of the matrix are $\mathtt{ev}(\rho_B) = \{0,1\}$, so the entropy of B equals

$$H(\rho_B) = -0\log_2 0 - 1\log_2 1 = 0$$

The entropy of ρ_B is equal to zero, as expected, so there is no surprisal regarding the result of the measurement of qubit B. However, if we calculate the reduced density matrix of A, we find that it is

$$\rho_A = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{52}$$

Thus, $H(\rho_A) = -(1/2)\log_2(1/2) - (1/2)\log_2(1/2) = 1$; so the surprisal is 1 bit, the largest it can possibly be.

The conditional entropy of a density matrix can be calculated using the partial trace of its reduced density matrix as explained below.

Definition. *Let ρ_{AB} be a bipartite density matrix. The* ***conditional von Neumann entropy of A given B****, denoted $H(A|B)$, is equal to*

$$H(A|B) = H(\rho_{AB}) - H(\mathrm{Tr}_A\,\rho_{AB}) = H(\rho_{AB}) - H(\rho_B) \tag{53}$$

Example 10. Let $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, one of the entangled Bell states, and let $\rho_{AB} = |\Phi^+\rangle\langle\Phi^+|$ be the density matrix describing a bipartite quantum system. Since ρ_{AB} only consists of one pure state, $H(\rho_{AB}) = 0$. However, calculating the partial trace over A of ρ_{AB} yields

$$\rho_B = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| \tag{54}$$

It follows from (54) that ρ_B is a mixed state consisting of the pure states $|0\rangle$ and $|1\rangle$ both with probabilities $1/2$. Thus, $H(\rho_B) = -\log_2(1/2) = 1$. This leads to the remarkable conclusion that

$$H(A|B) = H(\rho_{AB}) - H(\rho_B) = -1 \tag{55}$$

The fact that the conditional entropy of an entangled state is negative will be used in Chapter 5 in an effort to improve an entropic uncertainty bound.

Similar to the joint entropy of two independent random variables, the entropy of a product state simplifies down to the sum of individual entropies. Let ρ_{AB} be a density matrix describing a bipartite system that is a product state ($\rho_{AB} = \rho_A \otimes \rho_B$ for some density matrices ρ_A, ρ_B). It can be derived that

$$H(\rho_A \otimes \rho_B) = H(\rho_A) + H(\rho_B) \tag{56}$$

It follows from (56) and the fact that $\mathrm{Tr}_A(\rho_A \otimes \rho_B) = \rho_B$ that

$$H(A|B) = H(\rho_{AB}) - H(\rho_B) = H(\rho_A) + H(\rho_B) - H(\rho_B) = H(\rho_A) \tag{57}$$

Independent discrete random variables X and Y result in $H(X|Y)$ reducing to simply $H(X)$, while a density matrix describing a bipartite product state ρ_{AB} follows the relation $H(A|B) = H(A)$. This connection between classical and quantum entropies can be seen for a few examples in Table 5.

Classical formula/relation	**Quantum analogue**
$H(X,Y) = -\sum_{x\in X}\sum_{y\in Y}\Pr(x,y)\log_2(\Pr(x,y))$	$H(\rho_{AB}) = -\sum_{\lambda\in \mathsf{ev}(\rho_{AB})}\lambda\log_2\lambda$
$H(Y) = -\sum_{y\in Y}\Pr(y)\log_2(\Pr(y))$	$H(\rho_B) = H(\mathrm{Tr}_A\,\rho_{AB})$
$H(X\|Y) = H(X,Y) - H(Y)$	$H(A\|B) = H(\rho_{AB}) - H(\rho_B)$
$H(X\|Y) = H(X)$ if X and Y are independent.	$H(A\|B) = H(A)$ for the state described by the density matrix ρ_{AB} if ρ_{AB} equals the tensor product of two density matrices.

Table 5: Several formulas and relations in classical information theory (the Shannon entropy) along with their quantum analogues (the von Neumann entropy). We let X and Y be two random variables and ρ_{AB} be a density matrix of a bipartite quantum system.

5 Bounding quantum entropies

In this section, we discuss bounds on the entropy of bipartite quantum systems that follow from general quantum-mechanical principles. Then we look at some concrete bipartite systems to verify that these bounds are always satisfied and also to see how closely they can be approached.

5.1 The Maassen-Uffink bound and its generalization for entangled states

In 1988, Massen and Uffink introduced a new type of uncertainty principle in quantum mechanics in which the uncertainties of a pair of conjugate observables are quantified in terms of the von Neumann entropy, rather than the standard deviation as in the more conventional approach [8]. Because of this, their uncertainty relation and its generalizations are now commonly referred to as the *Entropic Uncertainty Relations* (often abbreviated to EUR). The simplest such relation involves the Pauli operators `X` and `Z` for a qubit and says that the sum of the von Neumann entropies of these observables in an arbitrary state of a qubit exceeds a minimum value that depends only on these two observables and not on the particular state considered. More precisely, the *Maassen-Uffink uncertainty relation* for a qubit in the state $|\psi\rangle$ can be expressed by the inequality

$$H(A) + H(B) \geq -\log_2 c \tag{58}$$

where A and B are observables with eigenbases $\{|a_1\rangle, \ldots, |a_n\rangle\}$ and $\{|b_1\rangle, \ldots, |b_n\rangle\}$ respectively. The constant c is defined to be

$$c = \max_{1 \leq i,j \leq n} c_{ij}, \quad \text{where } c_{ij} = |\langle a_i \mid b_j \rangle|^2, i, j = 1, ..., n \tag{59}$$

Note that if the bases are in $\mathbb{C}^2$ and are mutually unbiased (as the bases `X` and `Z` of a qubit are), $-\log_2 c = -\log_2(1/2) = 1$. The entropy $H(A)$ depends on the state $|\psi\rangle$ that we are considering, and is equal to

$$H(A) = -\sum_{j=1}^{n} \Pr(\psi|a_j) \log_2(\Pr(\psi|a_j)) = -\sum_{j=1}^{n} |\langle \psi|a_j\rangle|^2 \log_2(|\langle \psi|a_j\rangle|^2) \tag{60}$$

where $\Pr(\psi|a_j)$ is the conditional probability that a measurement of the observable A on the state $|\psi\rangle$ yields the eigenvalue a_j. $H(B)$ is defined in a similar fashion.

Example 11. Let $|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}|1\rangle$ for $\theta \in [0, \pi]$. It follows by routine calculation that

$$\Pr(0|\psi) = \cos^2\frac{\theta}{2},\ \Pr(1|\psi) = 1 - \Pr(0|\psi) = \sin^2\frac{\theta}{2} \tag{61}$$

$$\Pr(+|\psi) = \frac{1}{2}\left(1 + \sin\theta\right),\ \Pr(-|\psi) = 1 - \Pr(+|\psi) = \frac{1}{2}\left(1 - \sin\theta\right) \tag{62}$$

By using (61) and (62) in (60) along with $A = \mathtt{X}$ or $A = \mathtt{Z}$, one finds that

$$H(\mathtt{Z}) = -\cos^2\frac{\theta}{2}\log_2\left(\cos^2\frac{\theta}{2}\right) - \sin^2\frac{\theta}{2}\log_2\left(\sin^2\frac{\theta}{2}\right) \tag{63}$$

$$H(\mathtt{X}) = -\frac{1}{2}(1+\sin\theta)\log_2\left(\frac{1+\sin\theta}{2}\right) - \frac{1}{2}(1-\sin\theta)\log_2\left(\frac{1-\sin\theta}{2}\right) \tag{64}$$

For the bases $\mathtt{X}$ and $\mathtt{Z}$, some simple calculations with their eigenstates shows that $-\log_2 c = 1$. Plotting $H(\mathtt{X}) + H(\mathtt{Z})$ and $-\log_2 c$ as a function of θ shows that (58) is satisfied everywhere in the interval $[0, \pi]$. The bound is satisfied as an equality when $\theta = 0$ or $\theta = \pi/2$, when $|\psi\rangle$ reduces to an eigenstate of $\mathtt{Z}$ or $\mathtt{X}$. In these two cases, there is total certainty about the outcome for one observable and total uncertainty about the outcome for the other. However, for an arbitrary state $|\psi\rangle$, there is an uncertainty about both observables and the total uncertainty can exceed the minimum by an appreciable amount.

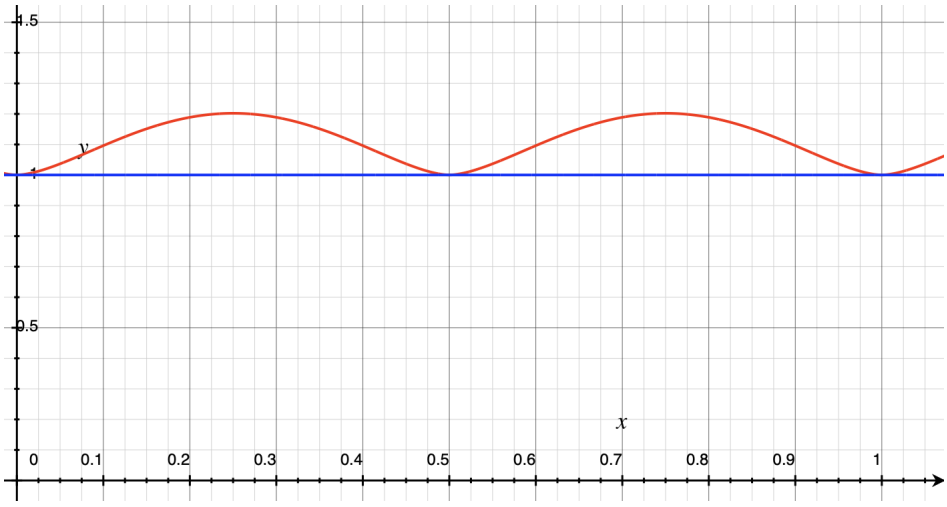

Figure 2: A plot of $H(\mathtt{X}) + H(\mathtt{Z})$ (in red) and $-\log_2 c$ (in blue) from Example 11 as a function of θ/π. The red line is greater than or equal to the blue line, so (58) is satisfied.

Berta et al. [2] strengthened the Maassen-Uffink relation (equation 58) in 2010 to incorporate the conditional entropy of A given B. If ρ_{AB} is the density matrix of the bipartite state, their relation states that

$$H(\mathtt{X} \mid B) + H(\mathtt{Z} \mid B) \geq -\log_2 c + H(A \mid B) \tag{65}$$

with c having the same meaning as in (59). The entropies on the left of (65) represent Bob's uncertainties about the results of Alice's measurements of $\mathtt{X}$ and $\mathtt{Z}$, while $H(A|B)$ represents Bob's uncertainty about Alice's state before Alice makes a measurement on it. Because Bob shares a partially entangled state with Alice, he has a partial knowledge about the results of Alice's measurements and this allows him to do better than permitted by (58). As we will see below, the entropy $H(A|B)$ is negative and it is the source of Bob's improved performance.

To calculate the entropies $H(\mathtt{X}|B)$ and $H(\mathtt{Z}|B)$ in (65), we need the joint density matrices of A and B after Alice makes a measurement of $\mathtt{X}$ or $\mathtt{Z}$ on her qubit. These density matrices are given by the expressions

$$\rho_{\mathtt{X}B} = |+\rangle\langle+| \otimes (\langle+| \otimes I_B)\,\rho_{AB}\,(|+\rangle \otimes I_B) + |-\rangle\langle-| \otimes (\langle-| \otimes I_B)\,\rho_{AB}\,(|-\rangle \otimes I_B) \tag{66}$$

$$\rho_{\mathtt{Z}B} = |0\rangle\langle 0| \otimes (\langle 0| \otimes I_B)\rho_{AB}(|0\rangle \otimes I_B) + |1\rangle\langle 1| \otimes (\langle 1| \otimes I_B)\,\rho_{AB}\,(|1\rangle \otimes I_B) \tag{67}$$

Since the value of c equals $\frac{1}{2}$ for the bases $\mathtt{X}$ and $\mathtt{Z}$, the bound simplifies to

$$H(\mathtt{X} \mid B) + H(\mathtt{Z} \mid B) \geq 1 + H(A \mid B) \tag{68}$$

A motivation for the strengthened form of the Maassen-Uffink relation in (65) is provided by the following guessing game to be played by two parties, Alice and Bob:

1. Bob creates a bipartite quantum system AB in a state described by the density matrix ρ_{AB}. He then sends qubit A to Alice and keeps qubit B for himself.
2. Alice chooses to measure either $\mathtt{X}$ or $\mathtt{Z}$ on her qubit and notes the eigenvalue obtained ($+1$ or -1).
3. Alice tells Bob which basis she measured in and challenges him to guess her outcome correctly.
4. Bob measures qubit B. He wins the guessing game if he correctly guesses Alice's outcome based on his measurement of B.

When Alice measures qubit A in Step 2, she collapses her qubit to an eigenstate of either the $\mathtt{X}$ or $\mathtt{Z}$ basis, resulting in the density matrix becoming either the density matrix in (66) or (67). The left-hand side of the inequality in (68) represents the total uncertainty Bob has about the result of Alice's measurement, considering that Alice could have measured in the $\mathtt{X}$ or $\mathtt{Z}$ basis.

The point of this game is to illustrate how Bob can use an entangled state between Alice and him to gain a "quantum advantage" in winning this game that allows him, in effect, to depress the lower bound on the right of (58). By analyzing this game, Berta et al. showed that the Maassen-Uffink relation in (58) can be replaced by the more general relation in (68).

We now work out the expressions for $\rho_{\mathtt{x}B}$, $\rho_{\mathtt{z}B}$, and ρ_B^A for the quantum game described above. The tensor product of the $m \times n$ matrix $A = \{a_{ij}\}_{1\leq i\leq m, 1\leq j\leq n}$ and the $p \times q$ matrix $B = \{b_{ij}\}_{1\leq i\leq p, 1\leq j\leq q}$ is defined as

$$A \otimes B = \begin{pmatrix} a_{11}B & \cdots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{m1}B & \cdots & a_{mn}B \end{pmatrix} \tag{69}$$

Denote ρ_{ij} to be the (i,j) entry of ρ_{AB} (for example, $\rho_{12} = \langle 00|\rho_{AB}|01\rangle$ and $\rho_{43} = \langle 11|\rho_{AB}|10\rangle$). Expanding the first term in the sum in (67) yields

$$\begin{aligned} &\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \otimes \left[\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \rho_{AB} \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 0 & 0 \end{pmatrix} \right] \\ &= \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \otimes \begin{pmatrix} \rho_{11} & \rho_{12} \\ \rho_{21} & \rho_{22} \end{pmatrix} \end{aligned} \tag{70}$$

Similarly, the second term in the sum in (67) can be simplified to get

$$\begin{aligned} &\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \otimes \left[\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \rho_{AB} \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} \right] \\ &= \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} \rho_{33} & \rho_{34} \\ \rho_{43} & \rho_{44} \end{pmatrix} \end{aligned} \tag{71}$$

The results of (70) and (71) substituted into (67) yield

$$\rho_{\mathtt{z}B} = \begin{pmatrix} \rho_{11} & \rho_{12} & 0 & 0 \\ \rho_{21} & \rho_{22} & 0 & 0 \\ 0 & 0 & \rho_{33} & \rho_{34} \\ 0 & 0 & \rho_{43} & \rho_{44} \end{pmatrix} \tag{72}$$

Similarly, we calculate $\rho_{\mathtt{X}B}$. The first term in the sum of (66) can be simplified to yield

$$\begin{aligned}
&\frac{1}{4}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \otimes \left[\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \rho_{AB} \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} \right] \\
&= \frac{1}{4}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \otimes \begin{pmatrix} \rho_{11}+\rho_{13}+\rho_{31}+\rho_{33} & \rho_{12}+\rho_{32}+\rho_{14}+\rho_{34} \\ \rho_{21}+\rho_{41}+\rho_{23}+\rho_{43} & \rho_{22}+\rho_{42}+\rho_{24}+\rho_{44} \end{pmatrix}
\end{aligned} \tag{73}$$

The second term in the sum in (66) can be simplified to get

$$\begin{aligned}
&\frac{1}{4}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \otimes \left[\begin{pmatrix} 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix} \rho_{AB} \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ -1 & 0 \\ 0 & -1 \end{pmatrix} \right] \\
&= \frac{1}{4}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes \begin{pmatrix} \rho_{11}-\rho_{31}-\rho_{13}+\rho_{33} & \rho_{12}-\rho_{32}-\rho_{14}+\rho_{34} \\ \rho_{21}-\rho_{41}-\rho_{23}+\rho_{43} & \rho_{22}-\rho_{42}-\rho_{24}+\rho_{44} \end{pmatrix}
\end{aligned} \tag{74}$$

The results of (73) and (74) substituted into (66) yield

$$\rho_{\mathtt{X}B} = \frac{1}{2}\begin{pmatrix} \rho_{11}+\rho_{33} & \rho_{12}+\rho_{34} & \rho_{31}+\rho_{13} & \rho_{32}+\rho_{14} \\ \rho_{21}+\rho_{43} & \rho_{22}+\rho_{44} & \rho_{41}+\rho_{23} & \rho_{42}+\rho_{24} \\ \rho_{31}+\rho_{13} & \rho_{32}+\rho_{14} & \rho_{11}+\rho_{33} & \rho_{12}+\rho_{34} \\ \rho_{41}+\rho_{23} & \rho_{42}+\rho_{24} & \rho_{21}+\rho_{43} & \rho_{22}+\rho_{44} \end{pmatrix} \tag{75}$$

We choose to denote the matrix $\mathrm{Tr}_A\, \rho_{AB}$ as ρ_B^A. The matrices $\rho_B^{\mathtt{X}}$ and $\rho_B^{\mathtt{Z}}$ can be calculated explicitly to get

$$\rho_B^{\mathtt{X}} = \rho_B^{\mathtt{Z}} = \begin{pmatrix} \rho_{11}+\rho_{33} & \rho_{12}+\rho_{34} \\ \rho_{21}+\rho_{43} & \rho_{22}+\rho_{44} \end{pmatrix} \tag{76}$$

This matches the reduced density matrix ρ_B^A:

$$\rho_B^A = \begin{pmatrix} \rho_{11}+\rho_{33} & \rho_{12}+\rho_{34} \\ \rho_{21}+\rho_{43} & \rho_{22}+\rho_{44} \end{pmatrix} \tag{77}$$

5.2 Verifications of the Berta relation for bipartite systems

In the following calculations, only ρ_B^A is computed for each density matrix, considering that $\rho_B^A = \rho_B^{\mathtt{X}} = \rho_B^{\mathtt{Z}}$ for the bipartite case. For this reason, all of these density matrices are referred to as ρ_B. We also denote the term $-\log_2 c = 1 = q_{MU}$, which is the *mutual information* between the two bases.

Example 12. A product state. Let $|\Psi_A\rangle$ and $|\Psi_B\rangle$ be the states

$$|\Psi_A\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle,\ \theta \in [0, \pi/2] \tag{78}$$

$$|\Psi_B\rangle = |0\rangle \tag{79}$$

The tensor product of these two states yields

$$|\Psi_{AB}\rangle = |\Psi_A\rangle \otimes |\Psi_B\rangle = \cos\theta|00\rangle + \sin\theta|10\rangle \tag{80}$$

The density matrix describing the system is therefore equal to $\rho_{AB} = |\Psi_{AB}\rangle\langle\Psi_{AB}|$. Expanding this expression and using (77) implies that

$$\rho_{AB} = \begin{pmatrix} \cos^2\theta & 0 & \sin\theta\cos\theta & 0 \\ 0 & 0 & 0 & 0 \\ \sin\theta\cos\theta & 0 & \sin^2\theta & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \tag{81}$$

$$\rho_B = \begin{pmatrix} \cos^2\theta + \sin^2\theta & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \tag{82}$$

It follows that

$$\mathtt{ev}(\rho_{AB}) = \{0, 0, 0, 1\}, \mathtt{ev}(\rho_B) = \{0, 1\} \tag{83}$$

Using formula (53), $H(A|B) = 0 - 0 = 0$. This shows that there is no "quantum advantage" to the traditional Maassen-Uffink bound. By (72),

$$\rho_{\mathtt{Z}B} = \begin{pmatrix} \cos^2\theta & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & \sin^2\theta & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \tag{84}$$

It follows that $\texttt{ev}(\rho_{\texttt{Z}B}) = \{\cos^2\theta, \sin^2\theta, 0, 0\}$, which means that

$$H(\texttt{Z}|B) = -\cos^2\theta \log_2(\cos^2\theta) - \sin^2\theta \log_2(\sin^2\theta) \tag{85}$$

Lastly, by (75),

$$\rho_{\texttt{X}B} = \frac{1}{2}\begin{pmatrix} 1 & 0 & \sin 2\theta & 0 \\ 0 & 0 & 0 & 0 \\ \sin 2\theta & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \tag{86}$$

It follows that $\texttt{ev}(\rho_{\texttt{X}B}) = \{0, 0, (1+\sin 2\theta)/2, (1-\sin 2\theta)/2\}$. Thus,

$$H(\texttt{X}|B) = -\frac{1}{2}(1+\sin(2\theta))\log_2\left(\frac{1+\sin(2\theta)}{2}\right) - \frac{1}{2}(1-\sin(2\theta))\log_2\left(\frac{1-\sin(2\theta)}{2}\right) \tag{87}$$

From these calculations,

$$\begin{aligned} H(\texttt{X}|B) + H(\texttt{Z}|B) - H(A|B) - q_{MU} = &-\frac{1}{2}(1+\sin 2\theta)\log_2\left(\frac{1+\sin 2\theta}{2}\right) \\ &-\frac{1}{2}(1-\sin 2\theta)\log_2\left(\frac{1-\sin 2\theta}{2}\right) \\ &-\cos^2\theta\log_2\left(\cos^2\theta\right) - \sin^2\theta\log_2\left(\sin^2\theta\right) - 1 \end{aligned} \tag{88}$$

Plotting (88) as a function of θ shows that (88) is always non-negative (see Figure 3). Thus, (68) holds for all $\theta \in [0, \pi]$. The bound is saturated (the difference between the two sides equal zero) when θ is a multiple of $\pi/4$.

When $\theta = \pi/4$, $|\Psi_A\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle = |+\rangle$. Therefore, the bound is saturated when $|\Psi_A\rangle$ is an eigenstate of $\texttt{X}$. When $\theta = \pi/2$, $|\Psi_A\rangle = |1\rangle$. Therefore, the bound is saturated when $|\Psi_A\rangle$ is an eigenstate of $\texttt{Z}$. However, for other values of θ, the bound is exceeded because the state is an eigenstate of neither of the observables ($\texttt{X}$ or $\texttt{Z}$) considered.

Example 13. An entangled state. Let $|\Psi_{AB}\rangle$ be the state

$$|\Psi_{AB}\rangle = \cos\theta|00\rangle + \sin\theta|11\rangle \text{ where } \theta \in (0, \pi/2) \tag{89}$$

One can verify using (20) that this state is entangled for all $\theta \in (0, \pi/2)$. The state becomes more and more entangled as θ nears $\pi/4$ (when $|\Psi_{AB}\rangle$ becomes a Bell state) and becomes less entangled as

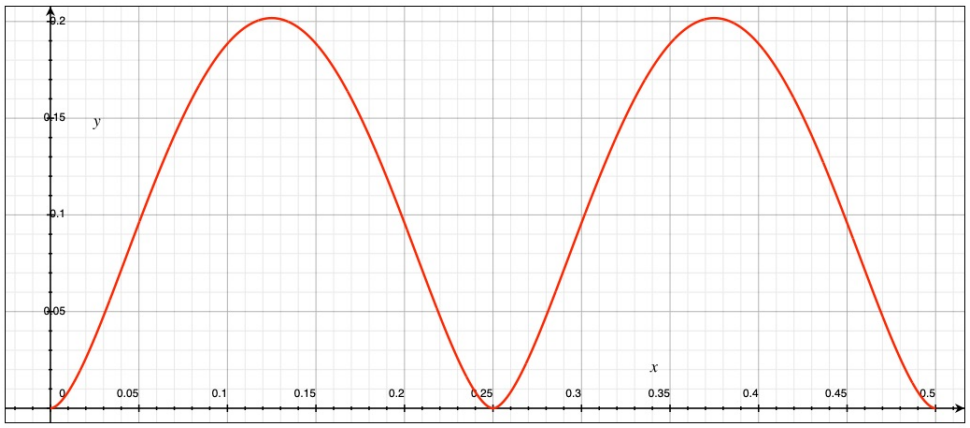

Figure 3: A plot of (88) as a function of θ/π.

θ moves further away from $\pi/4$. Note that $|\Psi_{AB}\rangle$ becomes the product state $|00\rangle$ and $|11\rangle$ at $\theta = 0$ and $\theta = \pi/2$ respectively, so the state becomes unentangled as θ approaches the boundaries of the open interval $(0, \pi/2)$. The density matrix describing the bipartite system is equal to $\rho_{AB} = |\Psi_{AB}\rangle\langle\Psi_{AB}|$. Expanding the density matrix and using (77) implies that

$$\rho_{AB} = \begin{pmatrix} \cos^2\theta & 0 & 0 & \sin\theta\cos\theta \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \sin\theta\cos\theta & 0 & 0 & \sin^2\theta \end{pmatrix} \tag{90}$$

$$\rho_B = \begin{pmatrix} \cos^2\theta & 0 \\ 0 & \sin^2\theta \end{pmatrix} \tag{91}$$

It follows that

$$\mathtt{ev}(\rho_{AB}) = \{0, 0, 0, 1\}, \mathtt{ev}(\rho_B) = \{\cos^2\theta, \sin^2\theta\} \tag{92}$$

Using formula (53), $H(A|B) = \cos^2\theta \log_2(\cos^2\theta) + \sin^2\theta \log_2(\sin^2\theta)$. Note that evaluating $H(A|B)$ for any value of $\theta \in (0, \pi/2)$ yields a **negative conditional entropy**. By (72),

$$\rho_{\mathtt{z}B} = \begin{pmatrix} \cos^2\theta & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \sin^2\theta \end{pmatrix} \tag{93}$$

It follows that $\mathtt{ev}(\rho_{\mathtt{Z}B}) = \{\cos^2\theta, \sin^2\theta, 0, 0\}$, which means that

$$H(\mathtt{Z}|B) = 0 \tag{94}$$

Lastly, by (75),

$$\rho_{\mathtt{X}B} = \frac{1}{2}\begin{pmatrix} \cos^2\theta & 0 & 0 & \cos\theta\sin\theta \\ 0 & \sin^2\theta & \cos\theta\sin\theta & 0 \\ 0 & \cos\theta\sin\theta & \cos^2\theta & 0 \\ \cos\theta\sin\theta & 0 & 0 & \sin^2\theta \end{pmatrix} \tag{95}$$

It follows that $\mathtt{ev}(\rho_{\mathtt{X}B}) = \{1/2, 1/2, 0, 0\}$. Thus,

$$H(\mathtt{X}|B) = 1 - \cos^2\theta\log_2(\cos^2\theta) - \sin^2\theta\log_2(\sin^2\theta) \tag{96}$$

From these calculations,

$$H(\mathtt{X}|B) + H(\mathtt{Z}|B) = 1 + H(A|B) \tag{97}$$

(97) shows that (68) is satisfied for all values of $\theta \in (0, \pi/2)$. The state in (89) has some entanglement for all θ in the interval $(0, \pi/2)$. This results in a negative value of $H(A|B)$, which causes the right-hand side of (97) to fall below 1; displaying the "quantum advantage" that allows Bob to do better than if he knew nothing about Alice's state. When $\theta = \pi/4$, $H(A|B) = -1$ and the right side of (97) drops to 0; Bob's uncertainty about the result of Alice's measurement then goes to 0 and he can win the game 100 percent of the time. This example shows clearly how Bob's probability of winning the game goes up from 50 percent (when he shares a product state with Alice) to 100 percent (when he shares a maximally entangled state).

Example 14. A Werner state. Let ρ_{AB} be a mixed state described by the density matrix

$$\rho_{AB} = \frac{1}{4}pI_4 + \left(1 - \frac{3p}{4}\right)|\Phi^+\rangle\langle\Phi^+|,\ p \in [0, 1] \tag{98}$$

where $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. This state represents a perfectly entangled state in the presence of noise, which increases as p increases. Writing ρ_{AB} as a 4×4 matrix and using (77) yields

$$\rho_{AB} = \frac{1}{4}\begin{pmatrix} 2-p & 0 & 0 & 2-2p \\ 0 & p & 0 & 0 \\ 0 & 0 & p & 0 \\ 2-2p & 0 & 0 & 2-p \end{pmatrix}, \quad \rho_B = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{99}$$

It follows that

$$\mathtt{ev}(\rho_{AB}) = \{p/4, p/4, p/4, 1-(3p/4)\}, \mathtt{ev}(\rho_B) = \{1/2, 1/2\} \tag{100}$$

Using formula (53),

$$H(A|B) = -\frac{3p}{4}\log_2\left(\frac{1}{4}p\right) - \left(1-\frac{3p}{4}\right)\log_2\left(1-\frac{3p}{4}\right) - 1 \tag{101}$$

By (72),

$$\rho_{\mathtt{z}B} = \frac{1}{4}\begin{pmatrix} 2-p & 0 & 0 & 0 \\ 0 & p & 0 & 0 \\ 0 & 0 & p & 0 \\ 0 & 0 & 0 & 2-p \end{pmatrix} \tag{102}$$

It follows that

$$\mathtt{ev}(\rho_{\mathtt{z}B}) = \{p/4, p/4, (2-p)/4, (2-p)/4\} \tag{103}$$

From (103), we find that

$$H(\mathtt{Z}|B) = -\left(1-\frac{1}{2}p\right)\log_2\left(\frac{1}{4}(2-p)\right) - \frac{1}{2}p\log_2\left(\frac{1}{4}p\right) - 1 \tag{104}$$

Lastly, by (75),

$$\rho_{\mathtt{x}B} = \frac{1}{4}\begin{pmatrix} 1 & 0 & 0 & 1-p \\ 0 & 1 & 1-p & 0 \\ 0 & 1-p & 1 & 0 \\ 1-p & 0 & 0 & 1 \end{pmatrix} \tag{105}$$

It follows that

$$\mathtt{ev}(\rho_{\mathtt{X}B}) = \{(2-p)/4, (2-p)/4, p/4, p/4\} \tag{106}$$

By (106),

$$H(\mathtt{X}|B) = -\left(1-\frac{1}{2}p\right)\log_2\left(\frac{2-p}{4}\right) - \frac{1}{2}p\log_2\left(\frac{1}{4}p\right) - 1 \tag{107}$$

From these calculations,

$$\begin{aligned} H(\mathtt{X}|B) + H(\mathtt{Z}|B) - H(A|B) - q_{MU} = & -(2-p)\log_2\left(\frac{1}{4}(2-p)\right) - p\log_2\left(\frac{1}{4}p\right) \\ & + \frac{3}{4}p\log_2\left(\frac{1}{4}p\right) + \left(1-\frac{3}{4}p\right)\log_2\left(1-\frac{3}{4}p\right) \end{aligned} \tag{108}$$

The plot of (108) as a function of p is shown in Figure 4. Note that when $p = 0$ and $p = 1$, (108) is equal to zero. Thus, the bound is saturated at $p = 0$ and $p = 1$ (which correspond to a perfectly entangled state and 100 percent noise, respectively). The difference listed in (108) is always non-negative, showing that (68) is satisfied for all values of $p \in [0, 1]$.

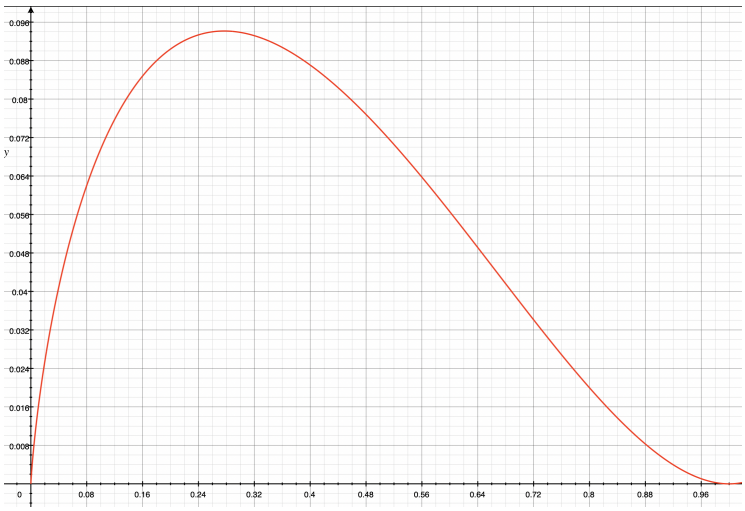

Figure 4: A plot of (108) as a function of p.

The saturation of the bound at $p = 0$ and $p = 1$ has different meanings. At $p = 0$, when Alice and Bob share a maximally entangled state, $H(A|B)$ cancels out q_{MU} and Bob's perfect knowledge of Alice's result allows him to win the game with absolute certainty. However, for $p = 1$, Bob's qubit is completely uncorrelated with Alice's and he has no more than a 50 percent probability of winning the game; the saturation in this case is due to the fact that $H(\mathtt{Z}|B) = H(\mathtt{X}|B) = H(A|B) = 1$, reflecting the complete

ignorance that Bob has of the state of Alice's qubit or the outcomes of her measurements of either `Z` or `X`. For other values of p, Bob's ignorance of Alice's result always outweighs his quantum advantage and so the plot in Figure 4 always stays above 0.

6 Conclusion

This report has investigated the Maassen-Uffink uncertainty relation along with its generalization formulated by Berta et al. The Maassen-Uffink relation deals with the uncertainty of two non-commuting observables of an arbitrary system and establishes a lower bound on the sum of their entropies for an arbitrary quantum state. Berta et al. showed how the Maassen-Uffink relation could be generalized to deal with a bipartite quantum state shared by two parties. This generalized version of the Maassen-Uffink relation was investigated in detail in this report due to its connection to quantum key exchange protocols involving two parties. The generalization by Berta et al. was studied for three types of bipartite states: (i) a product state, (ii) an entangled state with a variable amount of entanglement, and (iii) a perfectly entangled state contaminated by a variable amount of random noise. Case (i) demonstrates how a lack of entanglement in the bipartite state reduces Berta et. al's relation to the Maassen-Uffink relation. Case (ii) demonstrates how Maassen and Uffink's bound is improved by using an entangled state (even if it isn't maximally entangled) and case (iii) strengthens the claim that the Maassen-Uffink relation can be improved using a maximally entangled state.

One area that we did not touch upon but merits a full discussion is the formulation of *tripartite uncertainty relations*. Renes and Boulieau [10] generalized the Maassen-Uffink relation to deal with a three-qubit system. When qubits A, B, and C in a tripartite system are held by Alice, Bob, and Charlie respectively, the tripartite uncertainty relation bounds the sum of the information that Bob has about Alice's measurement of `X` on her qubit and the information Charlie has about Alice's measurement of `Z` on her qubit.

A further investigation of bipartite and tripartite uncertainty relations is carried out in a paper by Coles et. al [4], which also discusses its relevance for the security of quantum key distribution protocols. The topic of tripartite relations and its relevance for quantum key exchange could not be studied in this project and would be an area worth exploring further.

References

[1] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Phys. Rev. Lett.*, 70:1895–1899, Mar 1993.

[2] Mario Berta, Matthias Christandl, Roger Colbeck, Joseph M. Renes, and Renato Renner. The uncertainty principle in the presence of quantum memory. *Nature Physics*, 6(9):659–662, 2010.

[3] Cyril Branciard, Nicolas Gisin, Barbara Kraus, and Valerio Scarani. Security of two quantum cryptography protocols using the same four qubit states. *Physical Review A*, 72(3), Feb 2005.

[4] Patrick J. Coles, Mario Berta, Marco Tomamichel, and Stephanie Wehner. Entropic uncertainty relations and their applications. *Reviews of Modern Physics*, 89(1), 2017.

[5] Thomas M. Cover and Joy A. Thomas. *Entropy, Relative Entropy, and Mutual Information*, page 41. Wiley, 2 edition, 2005.

[6] Abdullah Al Hasib and Abul Ahsan Md. Mahmudul Haque. A comparative study of the performance and security issues of aes and rsa cryptography. 2:505–510, 2008.

[7] Susan Loepp and William Kent Wootters. *Protecting information: From classical error correction to quantum cryptography.* Cambridge University Press, 2006.

[8] Hans Maassen and J. B. M. Uffink. Generalized entropic uncertainty relations. *Phys. Rev. Lett.*, 60:1103–1106, Mar 1988.

[9] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information.* Cambridge University Press, 2019.

[10] Joseph M. Renes and Jean-Christian Boileau. Conjectured strong complementary information tradeoff. *Physical Review Letters*, 103(2), Jul 2009.

[11] Benjamin Schumacher and Michael D. Westmoreland. *Quantum processes, systems, and information.* Cambridge University Press, 2010.

[12] Claude E. Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 27(4):623–656, 1948.

[13] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1997.