Entropic uncertainty relations (EURs) and their connections to QKD protocols

Ethan Washock (MA, PH)
Advisor: Professor Padmanabhan K. Aravind (PH), Professor Herman Servatius (MA)

Introduction

- Shor's algorithm, which lets quantum computers factor large numbers more quickly than any classical computer, poses a threat to traditional cryptographic protocols.
- This threat to classical cryptography posed by quantum computers can be countered by using a new method for sharing a secret key based on the exchange of qubits. These protocols which rely on a secret key being encoded into a system of qubits are called **quantum key distribution (QKD) protocols**, and their security is ensured by the laws of quantum mechanics.
- Verifying the security of these protocols can be done using a measure of uncertainty called the **von Neumann entropy**, which is a generalization of the Shannon entropy used in classical information theory.

The BB84 Protocol

The BB84 protocol is the first QKD protocol. A sender Alice and receiver Bob follow this procedure:

1. Alice sends a key through a sequence of qubits, which are in eigenstates of the Pauli spin operators **X** and **Z**.
2. Bob measures either **X** or **Z** on each of Alice's qubits according to a random basis string.
3. Alice and Bob determine, using a public channel, which qubits they prepared or measured in the same basis, which allows them to generate a shared key.
4. Alice and Bob then use classic cryptographic techniques to shrink their key to a fraction of its original length to ensure that any information that may have leaked out to an eavesdropper has been shrunk to zero.

The virtue of BB84 is that any observation on the transmitted qubits is not passive and causes errors that can be detected and corrected in Step 4.

Background on entropy

The **Shannon entropy** of a random variable X, denoted H(X), is a measure of its uncertainty and can be thought of as the average number of yes or no questions that must be asked to determine the outcome of that variable.

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

Other types of entropy

The **joint entropy** characterizes the uncertainty of a pair of random variables, and can be used to calculate the **conditional entropy**, or uncertainty about one variable when given information about another.

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

$$H(X|Y) = H(X,Y) - H(Y)$$

These classical measures of uncertainty have analogues for qubits in which the role of the Shannon entropy is taken over by the **von Neumann entropy,** calculated by replacing the probabilities in the Shannon entropy by the eigenvalues of the density matrix describing the quantum system.

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

Several formulas in classical information theory along with their quantum analogues.

Entropic uncertainty relations

- Maassen and Uffink formulated a bound on the sum of entropies of two conjugate bases for a quantum state. This sum is bounded by a function of *c*, which is a measure of the closest distance between an eigenstate of A and one of B.

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

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

A strengthened EUR

Berta et al. strengthened the Maassen-Uffink relation to incorporate the conditional entropy of A given B.

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

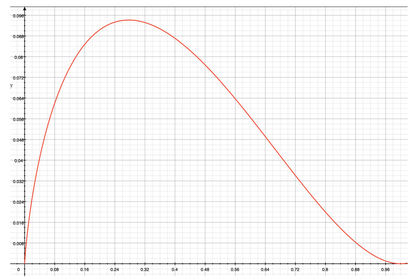
The entropies on the left represent Bob's uncertainties about the results of Alice's measurements of **X** and **Z**, while H(A|B) represents Bob's uncertainty about Alice's state before Alice makes a measurement on it.

The use of an entangled state allows for H(A|B) to be negative (an occurrence that is impossible classically) and leads to the Maassen-Uffink bound being lowered.

We verified Berta's strengthened EUR for several types of bipartite states:

- A product state (analogous to independent variables in classical information theory)
- An entangled state with variable entanglement
- A Werner state (a perfectly entangled state with noise)

$$H(\mathtt{X}|B) + H(\mathtt{Z}|B) - H(A|B) - q_{MU}$$



The difference between the two sides of the Berta EUR for a Werner state as a function of noise.

$$\rho_{AB} = \frac{1}{4} p I_4 + \left(1 - \frac{3p}{4}\right) |\Phi^+\rangle\langle\Phi^+|, \; p \in [0,1]$$

$$|\Phi^+\rangle = \tfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Conclusion

- We verified Berta et al.'s strengthened EUR for three types of bipartite states.
- This study could be extended to cover tripartite EURs which are of relevance to QKD protocols involving an eavesdropper.

References

[1] P. Coles, M. Berta, M. Tomamichel, and S. Wehner. *Entropic uncertainty relations and their applications*. Reviews of Modern Physics, 89(1), 2017.
[2] H. Maassen and J. B. M. Uffink. *Generalized entropic uncertainty relations*. Phys. Rev. Lett., **60,** 1103, 1988.