Exercise 12.1 Entropic Uncertainty Relations

In this exercise, we will derive a particular entropic uncertainty relation that is useful for proving security of quantum key distribution protocols. To do this we will need a few intermediate steps.

a) *Show the following relation for the relative entropy $D(\rho||\sigma)$ that you encountered in the last exercise sheet:*

$$D(S||T) \geq D(S||\tilde{T}) \tag{1}$$

for all positive operators S, T and $\tilde{T}$ such that $\tilde{T} \geq T$.

We shall denote the Hilbert space on which S, T, and $\tilde{T}$ act as $\mathcal{H}_\mu$. Now, introduce an isomorphic Hilbert space $\mathcal{H}_\nu$, and consider the space $\mathcal{H} = \mathcal{H}_\mu \oplus \mathcal{H}_\nu$. Let $\{|\mu_j\rangle\}$ and $\{|\nu_j\rangle\}$ be orthonormal bases for the two spaces $\mathcal{H}_\mu$ and $\mathcal{H}_\nu$. Now introduce the TPCPM acting on operators on $\mathcal{H}$, $\mathcal{F} : S \to F_1 S F_1^\dagger + F_2 S F_2^\dagger$, with $F_1 = \sum_j |\mu_j\rangle\langle\mu_j|$ and $F_2 = \sum_j |\mu_j\rangle\langle\nu_j|$. Define $W := \tilde{T} - T$. Then

$$\begin{aligned} D(S||T) &= D(S \oplus 0||T \oplus W) && (2)\\ &\geq D(\mathcal{F}(S \oplus 0)||\mathcal{F}(T \oplus W)) && (3)\\ &= D(S \oplus 0||(T + W) \oplus 0) && (4)\\ &= D(S||\tilde{T}) && (5) \end{aligned}$$

b) *Show that if c is a positive constant, then $D(S||cT) = D(S||T) + \log 1/c$, if $TrS = 1$.*

This is straightforward:

$$\begin{aligned} D(S||cT) &= \mathrm{Tr}(S(\log S - \log(cT))) && (6)\\ &= \mathrm{Tr}(S(\log S - \log c - \log T)) && (7)\\ &= D(S||T) + \log(1/c)\mathrm{Tr}(S) && (8)\\ &= D(S||T) + \log 1/c && (9) \end{aligned}$$

c) *Prove the following entropic uncertainty relation for a tripartite pure state ρ_{ABC}:*

$$H(X|B) + H(Z|C) \geq \log \frac{1}{c(X,Z)}, \tag{10}$$

where $X = \{|X_j\rangle\langle X_j|\}$ and $Z = \{|Z_k\rangle\langle Z_k|\}$ are orthonormal bases corresponding to different measurements on system A, and $c = \max_{j,k} |\langle X_j|Z_k\rangle|^2$ is the maximum overlap between the bases.

Hint: *Describe the X measurement on A with the isometry $V_X = \sum_j |j\rangle \otimes X_j$ and consider the associated state $\tilde{\rho}_{XABC} = V_X \rho_{ABC} V_X^\dagger$.*

For a pure state ρ_{ABC} the proof goes as follows: First, we describe the X measurement on A with the isometry $V_X = \sum_j |j\rangle \otimes X_j$ and the associated state $\tilde{\rho}_{XABC} = V_X \rho_{ABC} V_X^\dagger$. Then, for this state

$$\begin{aligned} H(X|B) &= -H(X|AC) && (11)\\ &= D(\tilde{\rho}_{XAC}||\mathbb{1}_X \otimes \tilde{\rho}_{AC}) && (12)\\ &= D(V_X \rho_{AC} V_X^\dagger||V_X(\sum_j X_j \rho_{AC} X_j)V_X^\dagger) && (13)\\ &= D(\rho_{AC}||\sum_j X_j \rho_{AC} X_j) && (14)\\ &\geq D(\bar{\rho}_{ZC}||\sum_{j,k} |\langle X_j|Z_k\rangle|^2 Z_k \otimes \mathrm{Tr}_A\{X_j \rho_{AC}\}) && (15)\\ &\geq D(\bar{\rho}_{ZC}||c(X,Z)\mathbb{1} \otimes \rho_C) && (16)\\ &= \log(1/c(X,Z)) + D(\bar{\rho}_{ZC}||\mathbb{1} \otimes \rho_C) && (17)\\ &= \log(1/c(X,Z)) - H(Z|C), && (18) \end{aligned}$$

where we have used $\bar{\rho}_{ZC} := \sum_k Z_k \rho_{AC} Z_k$.

d) *How would you generalize this proof for arbitrary mixed states ρ_{ABC}?*
For arbitrary mixed states, we first need to purify the state in question to ρ_{ABCD}. Then, we can use the data processing inequality for the von Neumann entropy $H(X|C) \geq H(X|CD)$ as the very first step and then proceed as before:

$$\begin{aligned} H(X|B) &\geq H(X|BD) && (19) \\ &= -H(X|AC) && (20) \\ &= .... && (21) \end{aligned}$$

e) *In which cases is the uncertainty relation satisfied with equality?*
First of all, we need pure states ρ_{ABC}. Then, we are left with the following steps in the proof from part c) that we need to satisfy with equality:

(a) $D(\rho_{AB}|| \sum_j X_j \rho_{AB} X_j) \geq D(\bar{\rho}_{ZB}|| \sum_{j,k} |\langle X_j|Z_k\rangle|^2 Z_k \otimes \mathrm{Tr}_A\{X_j \rho_{AB}\})$
In this step, the inequality arises because we have made use of the data processing inequality This is related to reversibility of the particular CPTPM used in the proof corresponding to Z-measurement on party A: It is saturated if and only if there exists a CPTPM $\hat{\mathcal{E}}$ that undoes the action of the measurement CPTPM $\mathcal{E}$ on S and T, i.e.

$$(\hat{\mathcal{E}} \circ \mathcal{E})(S) = S \quad (22)$$

$$(\hat{\mathcal{E}} \circ \mathcal{E})(T) = T \quad (23)$$

(b) $D(\bar{\rho}_{ZB}|| \sum_{j,k} |\langle X_j|Z_k\rangle|^2 Z_k \otimes \mathrm{Tr}_A\{X_j \rho_{AB}\}) \geq D(\bar{\rho}_{ZB}||c(X,Z)\mathbb{1} \otimes \rho_B)$
In this step, we basically replaced each element $|\langle X_j|Z_k\rangle|^2$ in the sum by its maximum value $c(X,Z)$, and applied the property you proved in part a) of this exercise. Hence, in order to satisfy this step with equality, we first need that each element $|\langle X_j|Z_k\rangle|^2$ is actually equal to the maximum, meaning that the overlap between all bases respectively is the same. This is the property of so-called *mutually unbiased bases (MUB)*. Secondly, we need equality in the proof of a). This is obtained if the map F that occurs in the proof actually saturates the DPI, and so we need a reversibility condition as before.

Exercise 12.2 Entropic Uncertainty Relation: Examples

In the following exercise consider two people, Alice and Bob, who share a state ρ_{AB} and a third person Charlie has the purification of this in his system C. Therefore, the pure state ρ_{ABC} describes the shared state between the three people.

a) *First, show that the overlap is $c(X,Z) = 1/2$ between the X and Z Pauli-operator measurements, described by the bases $\{|+\rangle, |-\rangle\}$ and $\{|0\rangle, |1\rangle\}$ respectively.*

Clearly the overlaps are all the same, and so $c(X,Z) = |\langle +|0\rangle|^2 = |\langle -|0\rangle|^2 = |\langle +|1\rangle|^2 = |\langle -|1\rangle|^2 = 1/2$.

b) *If ρ_{AB} is a maximally entangled two-qubit state $\rho_{AB} = |\psi^+\rangle\langle\psi^+|$, where $|\psi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$, and Alice performs a X or Z measurement, show that no matter what state Charlie has, he has maximum uncertainty about Alice's post-measurement state.*

If we consider the uncertainty relation from the previous exercise, we have two relevant versions:

$$H(X|B) + H(Z|C) \geq \log \frac{1}{c(X,Z)}$$
$$H(Z|B) + H(X|C) \geq \log \frac{1}{c(X,Z)}.$$

First, let's consider the case where Alice does a Z-basis measurement. Then, either Alice gets 0 or 1 with equal probability. The post-measurement state is:

$$\frac{1}{2}(|00\rangle_{AB}\langle 00| + |11\rangle_{AB}\langle 11|) \otimes \rho_C.$$

From this state, we have $H(Z|B) = H(ZB) - H(B) = 1 - 1 = 0$. This means that the second uncertainty relation above reduces to $H(X|C) \geq 1$. Since ρ_{XC} is a CQ state, we know that $H(X|C) \leq 1$, and so $H(X|C) = 1$ is maximal.

When Alice does a X-basis measurement, the post-measurement state is

$$\frac{1}{2}(|++\rangle_{AB}\langle ++| + |--\rangle_{AB}\langle --|) \otimes \rho_C,$$

where we use the fact that $|\psi^+\rangle = 1/\sqrt{2}(|++\rangle + |--\rangle)$. Due to symmetry, we have the result of $H(Z|C) = 1$, which is maximal.

c) *Conceptually, if Alice and Bob do not share a pure state, could Charlie have any information about Alice's post-measurement state? What if Alice and Bob have a pure state that is not maximally entangled?*

To answer the first question, if Alice and Bob do not share a pure state, then Charlie could have a purification of that state. As a result, the entropies $H(X|B)$ and $H(Z|B)$ are now less than 1, and so Charlie could have some information about Alice's measurement outcomes.

For the second question, you would need a state that would result in $H(X|B) = H(Z|B) = 0$, which is pure, but that is not maximally entangled. Since this is not necessarily the case, then Charlie could have some information about Alice's post measurement state. A simple counter example to show this is the state $|000\rangle$.

You could also consider if there is a state that is pure, not maximally entangled, but has $H(X|B) = H(Z|B) = 0$, but it can be shown that no such state exists.

Exercise 12.3 Another uncertainty Relation

a) *Show that, for the setting as in Exercise 12.1, $H(ZB) = H(ZC)$. Use the fact that ρ_{ABC} is pure.*
For this, look at the following:

$$H(ZB) = H(B|Z) + H(Z) \text{ and} \tag{24}$$
$$H(ZC) = H(C|Z) + H(Z) \tag{25}$$

Now, if we consider a projective measurement in the Z-basis on the pure state ρ_{ABC}, it is clear that conditioned on $Z = z$, the reduced state on BC is also pure. Hence, straightforwardly, $H(B|Z) = H(C|Z)$.

b) *Use the results of Exercise 12.1 and part a) of this exercise to show the following uncertainty relation:*

$$H(X|B) + H(Z|B) \geq \frac{1}{c(X,Z)} + H(A|B) \tag{26}$$

Looking at Exercise 12.1, we see that we would need $H(A|B) = H(Z|B) - H(Z|C)$ in order to prove the above uncertainty relation. To prove this, rewrite

$$\begin{aligned} H(Z|B) - H(Z|C) &= H(ZB) - H(B) - H(ZC) + H(C) && (27)\\ &= H(ZB) - H(B) - H(ZC) + H(AB) && (28)\\ &= H(A|B) + H(ZB) - H(ZC) && (29)\\ &= H(A|B) && (30) \end{aligned}$$