Quantum Information Theory
Series 12

HS 12
Prof. R. Renner

Exercise 12.1 Entropic Uncertainty Relation

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 $\tilde{T} \geq T$.

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

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

$$H(X|B) + H(Z|C) \geq \log \frac{1}{c(X,Z)}, \tag{2}$$

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* $\tilde{\rho}_{XABC} = V_X \rho_{ABC} V_X^\dagger$.

d) How do you generalize this proof for arbitrary mixed states ρ_{ABC}?

e) In which cases is the uncertainty relation satisfied with equality?

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.

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.

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?

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.

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

$$H(X|B) + H(Z|B) \geq \log \frac{1}{c(X,Z)} + H(A|B). \tag{3}$$