Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Quantum Information Theory
Problem Set 10

Spring 2008
Prof. R. Renner

Problem 10.1 Classical Resource Inequalities

Envision a communication system of two partners Alice A and Bob B and an eavesdropper Eve E. The classical analog of an entangled bit is a secret bit shared between A and B, modeled by a probability distrubution P_{ABE}, such that

$$P_{ABE} = P_{AB} \cdot P_E, \qquad P_{AB}[A{=}i, B{=}j] = (Q)_{ij}, \qquad Q = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix}. \tag{1}$$

Furthermore, classical communication between A and B is insecure in that everything broadcasted over the channel will be heard by E. Prove the following lemma:

Lemma 1. *Given A and B share l secure bits and unlimited classical communication, they cannot create more than l secure bits.*

a) Calculate the mutual information $I(A : B|E) = H(A|E) - H(A|B, E)$ when A and B share l secure bits.

b) Explain why the lemma follows after we show that the mutual information $I(A : B|E)$ is non-increasing under local operations and classical communication (LOCC).

c) Show that creating local randomness cannot increase mutual information:

$$I(A, X : B|E) \leq I(A : B|E). \tag{2}$$

d) Show that deterministic local operations $A \mapsto f(A)$ cannot increase mutual information:

$$I(f(A) : B|E) \leq I(A : B|E). \tag{3}$$

e) Show that classical communication cannot increase mutual information:

$$I(A, A' : B, A'|E, A') \leq I(AA' : B|E). \tag{4}$$

Problem 10.2 One-time Pad

Consider three random variables: a message M, a secret key S and a ciphertext C. We want to encode M as a ciphertext C using S with perfect secrecy, that is $I(C : M) = 0$. After the transmission, we want to be able to decode the ciphertext: $H(M|C, S) = 0$. Show that this is only possible if the key contains at least as much randomness as the message, namely $H(S) \geq H(M)$. Give an optimal algorithm for encoding and decoding.