ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Quantum Information Theory
Series 13

HS 13
Dr. J.M. Renes

Exercise 13.1 One-time Pad

Consider three random variables: a message M, a secret key K and a ciphertext C. We want to encode M as a ciphertext C using K with perfect secrecy, so that no one can guess the message from the cipher: $I(C:M)=0$.
After the transmission, we want to be able to decode the ciphertext: someone that knows the key and the cipher should be able to obtain the message perfectly, i.e. $H(M|C,K)=0$.
Show that this is only possible if the key contains at least as much randomness as the message, namely $H(K)\geq H(M)$. Give an optimal algorithm for encoding and decoding.

Exercise 13.2 Secret Key Agreement

In this exercise, we find a lower limit on the correlation between the qubits shared by Alice and Bob, such that secret key agreement is still possible. We express the shared state in the Bell basis to simplify calculations. The basis vectors are given by the Bell states

$$|\Psi_{1,2}\rangle := \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle), \qquad |\Psi_{3,4}\rangle := \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle). \tag{1}$$

Furthermore, let us introduce an additional step in the algorithm right after sifting: Alice and Bob agree on one of four equiprobable operations $\{\mathbb{1}, X, iY, Z\}$ that they perform on their corresponding qubit. After performing, they forget which operation they have chosen.

a) Express the Pauli operators $X\otimes X$, $iY\otimes iY$ and $Z\otimes Z$ in the Bell basis.

b) What is the most general shared state ρ_{AB} after these operations have been applied? Hint: The matrix ρ_{AB} will have 3 degrees of freedom.

In the error-free case presented during the lecture, the shared state is $\rho_{AB}=|\Psi_1\rangle\langle\Psi_1|$ and we expect perfect correlation between the measurement results at Alice and Bob. Let us denote the probability of detecting anti-correlation when measuring on the $\{|0\rangle,|1\rangle\}$ or $\{|+\rangle,|-\rangle\}$ basis by ε^+ and $\varepsilon^\times$ respectively. Henceforth, we assume that $\varepsilon^+=\varepsilon^\times=\varepsilon$.

c) Find the projectors P^+ and $P^\times$ corresponding to anti-correlated measurement outcomes.

d) For given ε, find the two additional constraints imposed on ρ_{AB} by

$$\varepsilon = \mathrm{tr}(\rho_{AB}P^+) = \mathrm{tr}(\rho_{AB}P^\times). \tag{2}$$

In the worst case, the adversary, Eve, holds a purification ρ_{ABE} of ρ_{AB}. The secret key rate R is defined as the number of secret bits that can be generated per shared qubit asymptotically. For our symmetric problem, it is given by $R=I(A:B)-I(A:E)$. A secret key can be generated if and only if $R>0$.

e) Show that $R>0$ can only be achieved if and only if $S(A,B)<1$.

f) For given ε, there is one degree of freedom left in ρ_{AB}. Maximize $S(A,B)$ to get rid of it.

g) Find an upper limit on ε, such that we can still generate a secret key. Hint: You will either have to find ε numerically or give an approximation.