Petros Wallden
Mina Doosti
Marine Demarty

QCS 2023–24
February 8, 2024

Tutorial 3

Problem 1 Entropies of quantum states

Consider the four bipartite states (of systems A and B), whose representations in the computational basis are given by the following density matrices:

$$\rho_1 = \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}, \quad \rho_2 = \frac{1}{4}\begin{pmatrix} 1 & 0 & 0 & \sqrt{3} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \sqrt{3} & 0 & 0 & 3 \end{pmatrix}, \quad \rho_3 = \frac{1}{4}\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix},$$

$$\rho_4 = \frac{1}{4}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \rho_5 = \frac{1}{4}\begin{pmatrix} 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 \end{pmatrix}.$$

(a) For each state, compute the von Neumann entropies $S(A)$ and $S(B)$ of the reduced states, as well as the von Neumann entropy $S(A,B)$ of the whole state.

(b) For each state, compute the conditional quantum entropy $S(A \mid B) = S(A,B) - S(B)$ and the quantum mutual information $S(A:B) = S(A) + S(B) - S(A,B)$.

(c) Use the definitions of the tensor product and what you know about projections and pure states in order to rewrite each of the bipartite states in a simplified form. Discuss how these relate to the results obtained in (a) and (b).

Problem 2

(a) Compute the secret key rate R of a QKD protocol given the probability that the sent qubits are detected is $Q = 1/3$, the error as a result of classical post-processing is $\xi = 1/3$, the penalty for using Holevo quantities is $\Delta(n,\varepsilon) = 1/10$, and given the following von Neumann entropies:

$$S(\rho^A) = \frac{1}{3}, \quad S(\rho^B) = \frac{1}{4}, \quad S(\rho^{AB}) = \frac{1}{12}, \quad S(\rho^E) = \frac{1}{5}, \quad S(\rho^{AE}) = \frac{7}{15}.$$

(b) What is the secret key rate if the QKD protocol in use is BB84 and we instead assume perfect detection, no finite-size effects, ideal classical post-processing, an average error in the $\{|0\rangle, |1\rangle\}$ basis of $e_b = 1/16$, and an average error in the $\{|+\rangle, |-\rangle\}$ basis of $e_p = 1/8$?

Problem 3

Alice sends to Bob one out of two possible states, depending on the outcome of tossing a fair coin. If the outcome is heads, then Alice sends $\rho_H = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$. If the outcome is tails, then Alice sends $|1\rangle$. Using the Holevo bound, determine an upper bound on the accessible information that Bob can obtain.

Problem 4

(a) Consider a secret bit string (random variable) X with outcomes in $\{0,1\}^{15}$ and a 2-universal family of hash functions $H = \{h_i\}_i$, where $h_i = h(i,\cdot)$ with $h\colon \mathcal{S}\times\{0,1\}^{15} \to \{0,1\}^3$. Using the leftover hash lemma, determine the maximum number of allowed leaked bits t of X such that, after using privacy amplification with the family of functions H, we produce a bit string that is ε-close to uniformly distributed in statistical distance, where $\varepsilon = 2^{-4}$. That is, such that $\delta[(h_i(x), i), (u, i)] \le 2^{-4}$.

(b) Prove that the family of functions $H = \{h_{a,b}\}_{a,b}$ is 2-universal, where $h_{a,b}\colon \mathbb{Z}_p \to \mathbb{Z}_p$ for p prime and $(a,b) \in \mathbb{Z}_p \times \mathbb{Z}_p$ is defined by

$$h_{a,b}(x) \equiv ax + b \pmod{p}.$$

Problem 5

Compute the secret key rate R_6 for the 6-state protocol given that the quantum bit error rate (QBER) is $D'_a = 1/8$.