Petros Wallden
Sean Thrasher
Laura Lewis

Tutorial 3: Solutions

QCS 2024–25
February 28, 2025

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.

Solution. Let us consider only ρ_2 as an example. Calculations for the other states are similar.

The state ρ_2 can also be written in Dirac notation as

$$\rho_2 = \frac{1}{4}\left|00\right\rangle\left\langle 00\right| + \frac{\sqrt{3}}{4}\left|00\right\rangle\left\langle 11\right| + \frac{\sqrt{3}}{4}\left|11\right\rangle\left\langle 00\right| + \frac{3}{4}\left|11\right\rangle\left\langle 11\right|.$$

Applying the definition of partial trace, we find the reduced state of each system

$$\begin{aligned}
\rho_2^A &= \operatorname{tr}_B \rho_2 \\
&= \frac{1}{4}\left|0\right\rangle\left\langle 0\right|\left\langle 0|0\right\rangle + \frac{\sqrt{3}}{4}\left|0\right\rangle\left\langle 1\right|\left\langle 1|0\right\rangle + \frac{\sqrt{3}}{4}\left|1\right\rangle\left\langle 0\right|\left\langle 0|1\right\rangle + \frac{3}{4}\left|1\right\rangle\left\langle 1\right|\left\langle 1|1\right\rangle \\
&= \frac{1}{4}|0\rangle\langle 0| + \frac{3}{4}|1\rangle\langle 1|, \\
\rho_2^B &= \operatorname{tr}_A \rho_2 \\
&= \frac{1}{4}\left\langle 0|0\right\rangle\left|0\right\rangle\left\langle 0\right| + \frac{\sqrt{3}}{4}\left\langle 1|0\right\rangle\left|0\right\rangle\left\langle 1\right| + \frac{\sqrt{3}}{4}\left\langle 0|1\right\rangle\left|1\right\rangle\left\langle 0\right| + \frac{3}{4}\left\langle 1|1\right\rangle\left|1\right\rangle\left\langle 1\right| \\
&= \frac{1}{4}|0\rangle\langle 0| + \frac{3}{4}|1\rangle\langle 1|.
\end{aligned}$$

Computing the von Neumann entropies for these states, we obtain

$$\begin{aligned}
S(A) = S(B) &= -\left(\frac{1}{4}\log\frac{1}{4} + \frac{3}{4}\log\frac{3}{4}\right) \\
&= -\left(-\frac{1}{2} + \left[\frac{3}{4}\log 3 - \frac{3}{2}\right]\right) \\
&= 2 - \frac{3}{4}\log 3 \approx 0.811.
\end{aligned}$$

Diagonalising ρ_2, we find it has a single nonzero eigenvalue, and this eigenvalue is equal to 1. The von Neumann entropy of the whole state ρ_2 is therefore

$$S(A,B) = -1\log 1 = 0.$$

Entropies of the other states are in accordance with the following table.

State	$S(A)$	$S(B)$	$S(A,B)$
ρ_1	1	1	0
ρ_2	$2-\frac{3}{4}\log 3 \approx 0.811$	$2-\frac{3}{4}\log 3 \approx 0.811$	0
ρ_3	1	1	1
ρ_4	1	1	2
ρ_5	0	0	0

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

Solution. Inserting the previously calculated entropies into the definitions given for $S(A \mid B)$ and $S(A:B)$ gives the following table.

State	$S(A)$	$S(B)$	$S(A,B)$	$S(A \mid B)$	$S(A:B)$
ρ_1	1	1	0	-1	2
ρ_2	$2-\frac{3}{4}\log 3$	$2-\frac{3}{4}\log 3$	0	$\frac{3}{4}\log 3 - 2$	$4-\frac{3}{2}\log 3$
ρ_3	1	1	1	0	1
ρ_4	1	1	2	1	0
ρ_5	0	0	0	0	0

(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).

Solution. Each of the states can be simplified in Dirac notation to be written as

$$\begin{aligned}
\rho_1 &= |\Phi^+\rangle\langle\Phi^+|\,,\\
\rho_2 &= \left(\frac{1}{2}|00\rangle + \frac{\sqrt{3}}{2}|11\rangle\right)\left(\frac{1}{2}\langle 00| + \frac{\sqrt{3}}{2}\langle 11|\right),\\
\rho_3 &= \frac{1}{2}(|{+}{+}\rangle\langle{+}{+}| + |{-}{-}\rangle\langle{-}{-}|),\\
\rho_4 &= \frac{1}{4}(\mathbb{1}\otimes\mathbb{1}),\\
\rho_5 &= |+\rangle\langle+| \otimes |-\rangle\langle-|\,.
\end{aligned}$$

The state ρ_1 is actually one of the Bell states, which confirms that ρ_1 is pure and $S(A,B)$ is zero. Notice that the conditional entropy of ρ_1 is negative. As opposed to classical probability distribution, where the conditional entropy is always positive, quantum states can have a negative conditional entropy, which is a clear signature of the non-classicality of the state. Observe also that the mutual information for ρ_4 is equal to 2. This is impossible classically, and is related to the fact that it is possible to communicate 2 bits of classical information by transmitting only a single qubit: so-called "superdense coding". Remark that the state ρ_3 is equivalent to a perfectly correlated coin in the $|\pm\rangle$ basis, whereas ρ_4 is equivalent to two uncorrelated unbiased coins in the computational basis. Finally, ρ_5 corresponds to the tensor product of two uncorrelated local pure states.

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:

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

Solution. We compute the secret key rate using the general formula

$$R = \frac{Q}{2}(\xi \cdot H(A : B) - S(A : E) - \Delta(n, \epsilon)).$$

We first compute the mutual information quantities

$$H(A : B) = S(\rho^A) + S(\rho^B) - S(\rho^{AB}),$$
$$S(A : E) = S(\rho^A) + S(\rho^E) - S(\rho^{AE}).$$

In our case we obtain

$$H(A : B) = \frac{1}{3} + \frac{1}{4} - \frac{1}{12} = \frac{1}{2},$$
$$S(A : E) = \frac{1}{3} + \frac{1}{5} - \frac{7}{15} = \frac{1}{15}.$$

Therefore, we obtain

$$R = \frac{1}{2} \cdot \frac{1}{3} \left(\frac{1}{3} \cdot \frac{1}{2} - \frac{1}{15} - \frac{1}{10} \right) = 0.$$

(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 $e_p = 1/8$?

Solution. We compute the secret key rate using the simplified formula for the BB84 protocol:

$$R_{BB84} = \frac{1}{2}(1 - h(e_b) - h(e_p)).$$

We first compute the binary entropy quantities

$$\begin{aligned} h(e_b) &= -e_b \log_2(e_b) - (1-e_b)\log_2(1-e_b) \\ &= -\frac{1}{16}\cdot(-4) - \frac{15}{16}\log_2\frac{15}{16} \approx 0.337, \\ h(e_p) &= -e_p \log_2 e_p - (1-e_p)\log_2(1-e_p) \\ &= -\frac{1}{8}\cdot(-3) - \frac{7}{8}\log_2\frac{7}{8} \approx 0.544. \end{aligned}$$

Therefore, we obtain

$$R_{BB84} \approx \frac{1}{2}(1-0.337-0.544) = 0.060.$$

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.

Solution. Alice prepares $\rho_H = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$ with probability $p_H = 1/2$ and $\rho_T = |1\rangle\langle 1|$ with probability $p_T = 1/2$. Bob's state is then

$$\begin{aligned} \rho &= p_H\rho_H + p_T\rho_T \\ &= \frac{1}{2}|1\rangle\langle 1| + \frac{1}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1| \\ &= \frac{1}{4}|0\rangle\langle 0| + \frac{3}{4}|1\rangle\langle 1| \\ &= \frac{1}{4}\begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix}. \end{aligned}$$

The accessible information by Bob is bounded by the Holevo quantity

$$I_{\text{acc}}(X:Y) \leq S(\rho) - p_H S(\rho_H) - p_T S(\rho_T).$$

We first determine $S(\rho)$. We compute the eigenvalues of ρ by solving

$$0 = \det(\rho - \lambda I) = \begin{vmatrix} \frac{1}{4}-\lambda & 0 \\ 0 & \frac{3}{4}-\lambda \end{vmatrix} = \left(\frac{1}{4}-\lambda\right)\left(\frac{3}{4}-\lambda\right).$$

Thus $\lambda_1 = 1/4$ and $\lambda_2 = 3/4$. The von Neumann entropy of ρ is then

$$S(\rho) = -\lambda_1\log_2\lambda_1 - \lambda_2\log_2\lambda_2 = -\frac{1}{4}\cdot(-2) - \frac{3}{4}\log_2\frac{3}{4} \approx 0.811.$$

For ρ_H, note that this is the maximally mixed qubit state, which gives the maximum value for the von Neumann entropy $S(\rho_H) = \log_2 2 = 1$ For ρ_T, since it is a pure state, we know that $S(\rho_T) = 0$. Finally, the Holevo bound gives us

$$I_{\text{acc}}(X:Y) \leq -\frac{3}{4}\log_2\frac{3}{4} \approx 0.311.$$

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 $\delta[(h_i(x), i), (u, i)] \leq 2^{-4}$.

Solution. Using the leftover hash lemma, we know that if we satisfy the condition

$$m \leq n - t - 2\log_2 \frac{1}{\varepsilon},$$

then we have

$$\delta[(h_i(x), i), (u, i)] \leq \varepsilon.$$

In our case, in which $m = 3$, $n = 15$, and $\varepsilon = 2^{-4}$, the condition becomes

$$t \leq n - m - 2\log_2 \frac{1}{\varepsilon} = 15 - 3 - 2 \cdot 4 = 4.$$

(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

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

Solution. Consider two distinct inputs $x_1, x_2 \in \mathbb{Z}_p$. For any two possible outputs $t_1, t_2 \in \mathbb{Z}_p$, we first want to compute the probability that both

$$h_{a,b}(x_1) \equiv t_1 \pmod{p},$$
$$h_{a,b}(x_2) \equiv t_2 \pmod{p}.$$

Substituting the definition of $h_{a,b}$, these are equivalent to

$$ax_1 + b \equiv t_1 \pmod{p},$$
$$ax_2 + b \equiv t_2 \pmod{p}.$$

Subtracting these relations, we get

$$a(x_2 - x_1) \equiv t_2 - t_1 \pmod{p}.$$

Since $x_2 \neq x_1$ (and so $x_2 - x_1 \neq 0$) and p is prime, we know $x_2 - x_1$ has a modular multiplicative inverse denoted $(x_2 - x_1)^{-1}$, and thus

$$a \equiv (t_2 - t_1)(x_2 - x_1)^{-1} \pmod{p}.$$

Using this a, we can find b by rearranging either of the initial relations. For example, using the first relation,

$$b \equiv t_1 - ax_1 \pmod{p}.$$

We have now constructed a unique key (a, b) such that $h_{a,b}(x_1) \equiv t_1$ and $h_{a,b}(x_2) \equiv t_2$. Thus, we have the probability

$$\Pr_{(a,b)\in\mathbb{Z}_p\times\mathbb{Z}_p}[h_{a,b}(x_1) \equiv t_1 \wedge h_{a,b}(x_2) \equiv t_2] = \frac{1}{p^2}.$$

Regarding the uniformity property, we need to prove that for a fixed $x \in \mathbb{Z}_p$ and for (a, b) sampled at random from $\mathbb{Z}_p \times \mathbb{Z}_p$,

$$\Pr_{(a,b)\in\mathbb{Z}_p\times\mathbb{Z}_p}[h_{a,b}(x) \equiv t] = \frac{1}{p}.$$

for all outputs t. Substituting the definition of $h_{a,b}$, this is equivalent to

$$\Pr_{(a,b)\in\mathbb{Z}_p\times\mathbb{Z}_p}[ax + b \equiv t] = \frac{1}{p}.$$

We can see that for any possible value of $a \in \mathbb{Z}_p$, there exists a unique b such that $ax + b \equiv t$, namely $b \equiv t - ax$. Therefore,

$$\Pr_{(a,b)\in\mathbb{Z}_p\times\mathbb{Z}_p}[ax + b \equiv t] = \frac{p}{p^2} = \frac{1}{p}.$$

Finally, if we combine the uniformity property with the first property above, we obtain the pairwise independence condition

$$\begin{aligned}\Pr_{(a,b)\in\mathbb{Z}_p\times\mathbb{Z}_p}[h_{a,b}(x_1) \equiv t_1 \wedge h_{a,b}(x_2) \equiv t_2] &= \frac{1}{p^2} \\ &= \frac{1}{p} \cdot \frac{1}{p} \\ &= \Pr_{(a,b)\in\mathbb{Z}_p\times\mathbb{Z}_p}[h_{a,b}(x_1) \equiv t_1] \cdot \Pr_{(a,b)\in\mathbb{Z}_p\times\mathbb{Z}_p}[h_{a,b}(x_2) \equiv t_2].\end{aligned}$$

Problem 5

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

Solution. We use the secret key rate formula specific to the 6-state protocol:

$$R_6 = \frac{1}{3}\left[1 + 3\frac{D'_a}{2}\log_2\frac{D'_a}{2} + \left(1 - \frac{3D'_a}{2}\right)\log_2\left(1 - \frac{3D'_a}{2}\right)\right].$$

Therefore, we obtain

$$R_6 = \frac{1}{3}\left[1 + 3 \cdot \frac{1}{16} \cdot (-4) + \frac{13}{16}\log_2\frac{13}{16}\right] \approx 0.0022.$$