Exercise 1. ***Quantum mutual information***

One way of quantifying correlations between two systems A and B is through their mutual information *$I(A:B)$.*

(a) Consider two qubits A and B in joint state ρ_{AB}.

(i) Prove that the mutual information of the Bell state $|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ is maximal. This is why we say Bell states are maximally entangled.

(ii) Show that $I(A:B) \leq 1$ for classically correlated states, $\rho_{AB} = p|0\rangle\langle 0|_A \otimes \sigma_B^0 + (1-p)|1\rangle\langle 1|_A \otimes \sigma_B^1$ (where $0 \leq p \leq 1$).

(b) Consider the so-called cat state *of four qubits, $A \otimes B \otimes C \otimes D$, that is defined as*

$$|\Phi\rangle = \frac{1}{\sqrt{2}}(|0000\rangle + |1111\rangle)\,. \tag{1}$$

Check how the mutual information between A and B changes with the knowledge of the remaining qubits, i.e compute

(i) $I(A:B)$,

(ii) $I(A:B|C)$,

(iii) $I(A:B|CD)$.

(c) Can you give an intuitive explanation for the results in (b)?

Solution.

(a) (i) The global state is pure and the reduced states on A and B are both fully mixed, $\rho_A = \rho_B = \mathbb{1}/2$, so we have

$$H(AB) = 0, \quad H(A) = H(B) = 1 \quad \Rightarrow \quad I(A:B) = H(A) + H(B) - H(AB) = 2,$$

which is maximal, because the entropy of a single qubit is at most $\log|\mathcal{H}_A| = 1$, as we saw in a previous exercise, and the entropy of the joint state is always non negative.

(ii) Notice that ρ_{AB} is a classical-quantum state. We can rewrite the mutual information as

$$I(A:B) = \underbrace{H(A)}_{\leq 1} - \underbrace{H(A|B)}_{\geq 0^{(*)}} \leq 1 \tag{S.1}$$

where $^{(*)}$ comes from Exercise 9.2 for classical-quantum states.

(b) The reduced states of the system for k qubits (which are independent of the qubits traced out) have entropies denoted by h_k, given as follows:

$$\begin{aligned}
\rho_4 &= |\Phi\rangle\langle\Phi| && \Rightarrow \quad h_4 = 0, \\
\rho_3 &= \frac{1}{2}(|000\rangle\langle 000| + |111\rangle\langle 111|) && \Rightarrow \quad h_3 = 1, \\
\rho_2 &= \frac{1}{2}(|00\rangle\langle 00| + |11\rangle\langle 11|) && \Rightarrow \quad h_2 = 1, \\
\rho_1 &= \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|) && \Rightarrow \quad h_1 = 1.
\end{aligned} \tag{S.2}$$

The mutual information between A and B given the knowledge of other qubits comes

$$\begin{aligned}
I(A:B) &= H(A) + H(B) - H(AB) = h_1 + h_1 - h_2 \\
&= 1, \\
I(A:B|C) &= H(A|C) + H(B|C) - H(AB|C) \\
&= H(AC) - H(C) + H(BC) - H(C) - H(ABC) + H(C) \\
&= h_2 - h_1 + h_2 - h_1 - h_3 + h_1 \\
&= 0, \\
I(A:B|CD) &= H(A|CD) + H(B|CD) - H(AB|CD) \\
&= H(ACD) - H(CD) + H(BCD) - H(CD) - H(ABCD) + H(CD) \\
&= h_3 - h_2 + h_3 - h_2 - h_4 + h_2 \\
&= 1\,.
\end{aligned} \tag{S.3}$$

(c) The results of the conditional mutual information can be interpreted as follows.

$I(A:B) = 1$ means that, upon getting system B, the entropy of A decreases by 1. This makes sense, since A and B are classically correlated, i.e. $\rho_{AB} = \frac{1}{2}(|00\rangle\langle 00| + |11\rangle\langle 11|)$ is the quantum representation of a clasical probability distribution between A and B, where they share the same bit (either both A and B are 0 or 1).

On the other hand, $I(A:B|C) = 0$ means that when being in possession of C, the entropy of A does not decrease when learning B. Again, this makes sense because A, B and C are classically correlated, $\rho_{ABC} = \frac{1}{2}(|000\rangle\langle 000| + |111\rangle\langle 111|)$.

Finally, $I(A:B|CD) = 1$ implies that when having access to CD already, the entropy of A still decreases by 1 when learning B. The situation here is different from the previous one because the total state on $ABCD$ has now quantum correlations. This means that when getting access to B, while already in possession of CD, we then have a maximally entangled state between A and BCD, whereas before we did not encounter this situation.

Exercise 2. *Classical and quantum Markov chains*

Three random variables X, Y, Z form a Markov chain *(also: have the* Markov property*), denoted by $X \leftrightarrow Y \leftrightarrow Z$, if $P_{Z|YX=x} = P_{Z|Y}$ for all $x \in \mathcal{X}$, the alphabet of X. In short we write $P_{Z|XY} = P_{Z|Y}$. One way of interpreting this is to say that once we know Y, we cannot learn more about Z when learning X.*

(a) *Show that the Markov property is symmetric, i.e. that it implies $P_{X|YZ=z} = P_{X|Y}$ for all $z \in \mathcal{Z}$.* Remark: *This is already suggested by the notation.*

(b) *Prove that for Markov chains the conditional mutual information is zero, $I(X:Z\,|\,Y) = 0$. This is a mathematical way of stating the interpretation mentioned above.*

For quantum states we can define the Markov property as follows. A state ρ_{ABC} on a tripartite Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$ is called a Markov state *if there exists a CPTP map $\mathcal{T}_{B\to BC}$ from B to BC s.t. $\rho_{ABC} = \mathcal{I}_A \otimes \mathcal{T}_{B\to BC}(\rho_{AB})$.*

(c) *Explain how this definition can be interpreted in the same way as the classical one.*

(d) *Prove that the GHZ state, the 3-qubit state $|\psi\rangle_{ABC} = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$, is not a Markov state by explicitly showing that a reconstruction map $\mathcal{T}_{B\to BC}$ cannot exist.*
Remark: *Please do not use (e) here.*

(e) *Prove that for quantum Markov states $I(A : C \,|\, B) = 0$.*
Hint: *Use strong subadditivity.*

Solution.

(a) We use the definition, denoted by $^{(*)}$ below, to prove this in a straight forward calculation:

$$P_{X|YZ} = \frac{P_{XYZ}}{P_{YZ}} = \frac{P_{Z|XY}P_{X|Y}P_Y}{P_{Z|Y}P_Y} \overset{(*)}{=} \frac{P_{Z|Y}P_{X|Y}}{P_{Z|Y}} = P_{X|Y}\,. \tag{S.4}$$

(b) Let $X \leftrightarrow Y \leftrightarrow Z$ be a Markov chain. We first show that then $H(X|YZ) = H(X|Y)$, where here H is the Shannon entropy. By definition of the Shannon entropy we have

$$\begin{aligned} H(X|YZ) &= -\sum_{x,y,z} P_{XYZ}(x,y,z) \log P_{X|YZ}(x\,|\,y,z) \\ &\overset{(*)}{=} -\sum_{x,y,z} P_{XYZ}(x,y,z) \log P_{X|Y}(x\,|\,y) \\ &= -\sum_{x,y} P_{XY}(x,y) \log P_{X|Y}(x\,|\,y) \\ &= H(X|Y)\,. \end{aligned} \tag{S.5}$$

Therefore:

$$I(X : Z|Y) = H(X|Y) - H(X|YZ) = H(X|Y) - H(X|Y) = 0\,. \tag{S.6}$$

(c) The classical interpretation is mentioned above: if $X \leftrightarrow Y \leftrightarrow Z$ form a Markov chain then knowing YZ is as good as knowing XYZ. In the definition for quantum Markov states this interpretation is directly used by saying that knowing the marginal state on AB is as good as knowing the whole state, because the total state on ABC can be reconstructed only from the marginal on AB. The map that does this reconstruction is $\mathcal{T}_{B\to BC}$.

(d) The marginal on AB of the GHZ state is $\rho_{AB} = \frac{1}{2}(|00\rangle\langle 00| + |11\rangle\langle 11|)$. A reconstruction map would have to achieve

$$\begin{aligned} \mathcal{I}_A \otimes \mathcal{T}_{B\to BC}(\rho_{AB}) &= \frac{1}{2}(|0\rangle\langle 0|_A \otimes \mathcal{T}_{B\to BC}(|0\rangle\langle 0|_B) + |1\rangle\langle 1|_A \otimes \mathcal{T}_{B\to BC}(|1\rangle\langle 1|_B) \\ &\overset{!}{=} \frac{1}{2}(|000\rangle\langle 000|_{ABC} + |000\rangle\langle 111|_{ABC} \\ &\quad + |111\rangle\langle 000|_{ABC} + |111\rangle\langle 111|_{ABC}) \\ &= |\psi\rangle\langle\psi|_{ABC}\,. \end{aligned} \tag{S.7}$$

Obviously the terms with $|0\rangle\langle 1|_A$ and $|1\rangle\langle 0|_A$ cannot be reconstructed with a map $\mathcal{T}$ of this form. Hence, $|\psi\rangle_{ABC}$ is not a Markov state.

(e) By strong subadditivity we know that always

$$I(A : C|B) = H(A|B) - H(A|BC) \geq H(A|B) - H(A|B) = 0\,. \tag{S.8}$$

For Markov states we know in addition that a CPTP map acting only on B can reconstruct ABC from AB only. Due to Stinespring such a CPTP map $\mathcal{T}_{B\to BC}$ can always be written as an isometry $V_{B\to BCE}$ followed by tracing out the additional system E, i.e. $\mathcal{T}_{B\to BC} = \mathrm{tr}_E \circ V_{B\to BCE}$. It is a fact that isometries do not change von Neumann entropy, so we must have $H(A|B) = H(A|BCE)$. On the other hand, again due to strong subadditivity, tracing out E in can only increase the conditional entropy: $H(A|BCE) \leq H(A|BC)$. Thus:

$$0 = H(A|BC) - H(A|BC) \geq H(A|BCE) - H(A|BC) = H(A|B) - H(A|BC) = I(A:C|B)\,. \tag{S.9}$$

Altogether this yields $I(A:C|B) = 0$ for quantum Markov states.

Remark: In fact, Petz' theorem states that a quantum state ρ_{ABC} is a Markov state if and only if $I(A:C|B) = 0$. The second part of this proof goes, however, beyond the scope of this lecture.