Summer Semester 2020
Markus Müller, Felix Binder, Andrew Garner
http://www.mpmueller.net/resource.html

Exercises - Week 5

Problem 5.1: Bell states and maximal entanglement (8 points)

The four Bell states form a basis for the Hilbert space of two qubits. In this exercise we will discover a reason why they are called 'maximally entangled'.

(i) Write down the four Bell states and consider local unitary operations of the form $U_{AB} = U_A \otimes U_B$. Can any Bell state converted into any other by such a local unitary operation? If no, provide a proof. If yes, specify a sufficient set of local unitary operations.

(ii) Can a product state $|\psi\rangle_{AB} = |a\rangle \otimes |b\rangle$ be obtained from a Bell state by a local unitary operation?

(iii) It is important to know that quantum teleportation does not permit faster than light communication. Proof this by showing that in the teleportation protocol introduced in the lecture, Bob does not obtain any information about Alice' input state $|\psi\rangle$ until she has communicated her measurement result. In no more than two sentences, state why your result is not in conflict with the functioning of quantum teleportation.

(iv) Show that Alice can use an extension of the teleportation protocol from the lecture to create any shared state $|\sigma\rangle_{AB}$ between her laboratory and Bob's by using one shared Bell state $|\phi^+\rangle$.
Hint: Consider Alice and Bob to start with the initial state $|\sigma\rangle_{12} \otimes |\phi^+\rangle_{AB}$ where Alice controls laboratories 1, 2, and A; Bob controls laboratory B. As in the original teleportation protocol encountered in the lecture, Alice and Bob may only perform measurements and unitary operations on systems in their control, as well as classical communication.

(v) We have called the Bell states 'maximally entangled'. Comment (briefly!) on how this terminology is justified for pure two-qubit states in light of what we have found out in this exercise.

Problem 5.2: Superdense coding, POVMs, and the Holevo bound (6+6 points)

In this exercise, to show the resource value of entanglement in superdense coding, we will address the following question: *How much classical information can be reliably communicated with a single qubit?*

Recall the defintion of a POVM:
A positive operator-valued measure (POVM) is a set of of positive operators $\{M_i\}$ *(i.e.,* $\langle v| M_i |v\rangle \geq 0 \; \forall \; i, |v\rangle$*) with* $\sum_i M_i = \mathbf{id}$.
The probability for obtaining outcome i when measuring a state ρ is given by $\mathrm{Tr}[M_i \rho]$. (Recall also that projective measurements are a special case of POVMs where the *POVM elements* M_i are given by orthogonal projectors $M_i = \Pi_i$, i.e., $\Pi_i \Pi_j = \delta_{i,j} \Pi_i$).

Now assume that with probability $p_x > 0$ Alice wants to send a message x to Bob. We can think of x as a realisation of a random variable X. Alice communicates each x by preparing and then sending a state ρ_x. For instance, she might toss a coin where x would be'heads' or 'tails'. To communicate the result of her toin coss Alice would send ρ_{heads} or ρ_{tails}, depending on her result. Bob then has to find out x by applying a POVM with elements M_y to the state that he receives.

(i) For a given ensemble $E_X = \{p_x, \rho_x\}$, and POVM $\{M_y\}$ with what probability will Bob measure the outcome y? What is the probability for him to measure y if Alice encoded x?

(ii) If Alice and Bob have complete freedom of agreeing a protocol in advance of communication, how many different values x can Alice encode in a d-dimensional quantum system such that Bob can decode them all perfectly reliably? Suggest one such optimal encoding and measurement strategy.
Remark: Answer this question without using the results from later parts of this exercise. You may of course make use of all previous results covered in this course.

Consider the maximum amount of (classical) information about X that Bob can recover by any POVM $\{M_y\}$. This is the accessible information:

$$I_{acc}(E_X) := \max_{\{M_y\}} I(X;Y)$$

where $I(X;Y)$ is the classical mutual information between Alice's random variable X, which she encodes in her quantum ensemble E_X, and Bob's random variable Y which he recovers from his POVM. The classical mutual information is a special case of the quantum mutual information $I(A;B)_\rho$ between two quantum systems A and B in the joint state ρ:

$$I(A;B)_\rho := S(A) + S(B) - S(AB)$$

where $S(A) = S(\mathrm{Tr}_B\,\rho)$, $S(B) = S(\mathrm{Tr}_A\,\rho)$, $S(AB) = S(\rho)$. We want to prove the *Holevo bound* $\chi(E_X) \geq I_{acc}(E_X)$ whith the *Holevo information* $\chi(E_X)$ given by:

$$\chi(E_X) := S\left(\sum_x p_x \rho_x\right) - \sum_x p_x S(\rho_x)$$

Important: parts (iii) to (v) are optional (+6 points)

(iii) (optional) As a first step, consider explicitly Alice' preparation procedure in terms of the following *classical-quantum state*:

$$\sigma_{CQ} = \sum_x p_x |x\rangle\langle x| \otimes \rho_x$$

and proof that $I(C;Q)_{\sigma_{CQ}} = \chi(E_X)$.

(iv) (optional) Proof the Holevo bound using following quantum data processing inequality which holds for all local operations of the form $\Lambda = \Gamma_A \otimes \Gamma_B$:

$$I(A;B)_\rho \geq I(A';B')_\sigma$$

where A' and B' are the output quantum systems and σ is the output state.

(v) (optional) Returning again to part (ii) of this problem, use the Holevo bound for an alternative proof of the maximum number of perfectly distinguishable messages.

Problem 5.3: QRTs from basic postulates (3 points)

In the lecture, we have stated the *free operations postulate (FOP)* as a postulate. In this exercise, we will show that it can in fact be derived from other basic postulates for quantum resource theories (QRTs), namely

(free creation of free states) The set of free states $\mathcal{F}$ is in one-to-one correspondence with the set of free creation maps $\Omega_c : \mathbb{C} \to \mathcal{H}$ ($\forall\, \mathcal{H}$).
In other words, ϕ is a free state if and only if $\mathcal{O}$ includes a free map $\Omega_c : \mathbb{C} \to \mathcal{H}$ with $\Omega_c(c_\phi) = \phi$ for some c_ϕ.

(free identity operations) For any permitted Hilbert space $\mathcal{H}$, the associated identity operation is a free operation: $\mathbf{id}_{\mathcal{H}} \in \mathcal{O}$,

(free concatenation of free operations) $\Omega, \Omega' \in \mathcal{O} \Rightarrow \Omega' \circ \Omega \in \mathcal{O}$, for all Ω and Ω' for which the output Hilbert space of Ω matches the input Hilbert space of Ω' and where $\circ$ stands for successive application.

(i) Write down the FOP. (ii) Then, derive it from the above.

Remark: We said in the lecture that there is a sense in which $\mathcal{O}$ is more fundamental for a QRT than $\mathcal{F}$. Note here that all postulates are on $\mathcal{O}$. $\mathcal{F}$ is only indirectly introduced via $\mathcal{O}$.

Problem 5.4: Resource theory of non-uniformity (8 points)

(i) For the QRT of non-uniformity, write down the the set of free states $\mathcal{F}_{nu}$ and the free operations – i.e., the set of (quantum) noisy operations $\mathcal{N}$.

(ii) For $\mathcal{O}_{c-max}$ induced by $\mathcal{F}_{nu}$ show that $\mathcal{N} \subseteq \mathcal{O}_{c-max}$.

(iii) What is the set $\mathcal{O}_{max}$ induced by $\mathcal{F}_{nu}$?

(iv) We know that $\mathcal{O}_{c-max} \subseteq \mathcal{O}_{max}$. For $\mathcal{F}_{nu}$, is it a strict subset, $\mathcal{O}_{c-max} \subset \mathcal{O}_{max}$, or are they equal $\mathcal{O}_{c-max} = \mathcal{O}_{max}$?

(v) For $\mathcal{F}_{nu}$, is $\mathcal{O}_{max}$ convex?