Quantum Information Theory
Problem Set 12

Spring 2008
Prof. R. Renner

Problem 12.1 Entanglement and Teleportation

Quantum teleportation from Alice A to Bob B can be described by a linear map $\mathcal{E}$ from operators on $\mathcal{H}_\mathrm{A}$ to operators on $\mathcal{H}_\mathrm{B}$, where $\mathcal{H}_\mathrm{A} = \mathcal{H}_\mathrm{B}$ are copies. In the lecture we showed that $\mathcal{E}[|\psi\rangle\langle\psi|] = |\psi\rangle\langle\psi|$ for all pure states $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.

a) Look at the state of the system after Alice's measurement but before she communicates her results to Bob. At this point, we know that Bob's state is in one of four possible states that are related to $|\psi\rangle$. Show that we still cannot extract any information on $|\psi\rangle$ out of Bobs state by calculating it as a probabilistic mixture of the four possible states. What is the physical relevance of this observation?

b) Show that the pure states span the space of Hermitian matrices.

c) Show that $\mathcal{E}[\rho] = \rho$, for any mixed state ρ. Furthermore, show that $(\mathcal{E} \otimes \mathbb{1}_\mathrm{R})[|\Psi\rangle\langle\Psi|] = |\Psi\rangle\langle\Psi|$, for any $|\Psi\rangle$ on $\mathcal{H}_\mathrm{A} \otimes \mathcal{H}_\mathrm{R}$. This implies that quantum teleportation preserves entanglement!

Problem 12.2 Optimality of Teleportation

We have previously shown that any physical teleportation algorithm (namely any teleportation algorithm that can be described by a trace-preserving CPM) will keep entanglement intact. Furthermore, we have introduced an algorithm that uses $n = 1$ EPR pairs and $m = 2$ bits of classical communication to teleport a quantum state between Alice (A) and Bob (B). We now have the tools necessary to show that this algorithm is optimal.

a) Show that $n \geq 1$ for any m.

It is not obvious why classical communication is needed from the above argument. Let us thus introduce a third party Charlie (C). Alice shares an EPR pair with Charlie and she intends to teleport her part of the pair to Bob.

b) Find $I'(B : C) - I(B : C)$ in this scenario, where $I(B : C)$ and $I'(B : C)$ is the mutual information between Bob and Charlie before respectively after the teleportation.

c) It is clear that local operations on A, B or C do not influence $I(B : C)$. If classical communication between A and B is allowed, show that $I'(B : C) - I(B : C) \leq m$.

We have shown that $n \geq 1$ and $m \geq 2$. The proposed algorithm is thus optimal.

Problem 12.3 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 $\rho_{\text{AB}} = |\Psi_1\rangle\langle\Psi_1|$ 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

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

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.

Problem 12.4 Bit Commitment

Someone proposes the following bit commitment protocol for a bit b: To commit, Alice generates a random string $X = \{0,1\}^n$ and encodes every bit into a qubit using a basis $B_0 = \{|0\rangle, |1\rangle\}$ if $b = 0$ or $B_1 = \{|+\rangle, |-\rangle\}$ if $b = 1$. These qbits are sent to Bob and he stores them. To unveil the bit, Alice sends b and X to Bob and he will validate the process by applying measurements on his states in basis B_b and comparing the results with X.

a) Show that Bob has no information about b before it is revealed, i.e. the protocol is concealing.

b) Show that if Alice commits honestly to 0, the probability of her unveiling a 1 without Bob noticing the cheat is equal to 2^{-n}.

c) Give a strategy that allows Alice to cheat perfectly, i.e. that allows her to unveil 0 or 1 in such a way that Bobs probability of detecting her cheating is zero.

Happy Holidays!