

**Exercise 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  $\mathcal{H}_A$  to operators on  $\mathcal{H}_B$ , where  $\mathcal{H}_A = \mathcal{H}_B$  are copies. In the lecture we showed that  $\mathcal{E}[|\psi\rangle\langle\psi|] = |\psi\rangle\langle\psi|$  for all pure states  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ .

- 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 Bob's state by calculating it as a probabilistic mixture of the four possible states. What is the physical relevance of this observation?
- Show that the pure states span the space of Hermitian matrices.
- Show that  $\mathcal{E}[\rho] = \rho$ , for any mixed state  $\rho$ . Furthermore, show that  $(\mathcal{E} \otimes \mathbb{1}_R)[|\Psi\rangle\langle\Psi|] = |\Psi\rangle\langle\Psi|$ , for any  $|\Psi\rangle$  on  $\mathcal{H}_A \otimes \mathcal{H}_R$ . This implies that quantum teleportation preserves entanglement!

**Exercise 12.2 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

$$|\Psi_{1,2}\rangle := \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle), \quad |\Psi_{3,4}\rangle := \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle). \quad (1)$$

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.

- Express the Pauli operators  $X \otimes X$ ,  $iY \otimes iY$  and  $Z \otimes Z$  in the Bell basis.
- What is the most general shared state  $\rho_{AB}$  after these operations have been applied? Hint: The matrix  $\rho_{AB}$  will have 3 degrees of freedom.

In the error-free case presented during the lecture, the shared state is  $\rho_{AB} = |\Psi_1\rangle\langle\Psi_1|$  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  $\varepsilon^+$  and  $\varepsilon^\times$  respectively. Henceforth, we assume that  $\varepsilon^+ = \varepsilon^\times = \varepsilon$ .

- Find the projectors  $P^+$  and  $P^\times$  corresponding to anti-correlated measurement outcomes.
- For given  $\varepsilon$ , find the two additional constraints imposed on  $\rho_{AB}$  by

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

In the worst case, the adversary, Eve, holds a purification  $\rho_{ABE}$  of  $\rho_{AB}$ . 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  $R > 0$ .

- Show that  $R > 0$  can only be achieved if and only if  $S(A, B) < 1$ .
- For given  $\varepsilon$ , there is one degree of freedom left in  $\rho_{AB}$ . Maximize  $S(A, B)$  to get rid of it.
- Find an upper limit on  $\varepsilon$ , such that we can still generate a secret key. Hint: You will either have to find  $\varepsilon$  numerically or give an approximation.