13 Basics of Information Theory

Exercises

13.1 Consider the encoding $AA \to 0$, $AB \to 10$ and $B \to 11$. Starting from a string of N_o messages show that the average number of messages strings used in for the encoding is given by $N_{AA} = N_o p^2/(1+p)$, $N_{AB} = N_o(1-p)p/(1+p))$, and $N_B = N_o(1-p)/(1+p)$. With the number of encoding steps given by $N_s = N_{AA} + N_{AB} + N_B$ show that the probabilities $p_{AA} = p^2$, $p_{AB} = p(1-p)$ annd $p_B = 1 - p$ follow.

13.2 Alice prepares messages A, B, and C with probabilities p_A, p_B, and p_C, respectively. Show that her messages contain maximum information for $p_A = p_B = p_C = 1/3$ and work out this maximum amount of information.

13.3 Alice creates messages A, B, C, and D. She chooses them with probabilities $p_A = 1/2$, $p_B = 1/4$ and $p_C = p_D = 1/8$. How much information is contained in one of her messages? Find an optimal bit-code for encoding these messages and show that in this code each bit has equal probability of having values 0 or 1.

13.4 Now imagine that Alice uses trits (with values 0,1,2) instead of bits to encode her messages and chooses to send A, B, C, D, and E with probabilities $p_A = p_B = 1/3$ and $p_C = p_D = p_E = 1/9$. What is an optimal code in this case? Show that in the optimal encoding each trit has equal probability of having values 0, 1, and 2.

13.5 Show that the conditional entropy $H(X|Y)$ is always larger than or equal to zero if local realism is assumed.

13.6 A communication channel transmits two messages A and B. With probability ℓ the two messages are swapped on the channel but otherwise transmitted faithfully. Calculate the channel capacity making use of its symmetry and show that the channel is ideal for $\ell = 0$ and $\ell = 1$.

14 Quantum Information

Exercises

14.1 Calculate the reduced density operator for each qubit of the Bell state $|\Psi^+\rangle$. Show that this result is the same for each Bell state and give a physical explanation. Use this to calculate the von Neumann entropy of a two qubit system in a Bell state as well as the reduced entropies of each of the qubits separately.

14.2 The density operator of two qubits A and B is given by $\rho_{AB} = (|\Psi^-\rangle\langle\Psi^-| + |\Phi^+\rangle\langle\Phi^+| + |\Psi^+\rangle\langle\Psi^+| + |\Phi^-\rangle\langle\Phi^-|)/4$. Calculate the von Neumann entropy $S(\rho_{AB})$ and the entropies of the reduced systems $S(\rho_A)$ and $S(\rho_B)$. Is the state ρ_{AB} entangled? If it is not entangled find the density operator ρ_{AB} in the form

$$\rho_{AB} = \sum_j p_j \rho_A^{(j)} \otimes \rho_B^{(j)}.$$

Repeat the above calculations for the state $\tilde{\rho}_{AB} = (|\Psi^-\rangle\langle\Psi^-| + |\Phi^+\rangle\langle\Phi^+|)/2$.

14.3 The density operator of a two qubit system is given by

$$\rho_{AB} = \rho_A \otimes \rho_B.$$

Show that the von Neumann entropy of this system is given by $S(\rho_{AB}) = S(\rho_A) + S(\rho_B)$.

14.4 Show that the conditional von Neumann entropy $S(\rho_A|\rho_B)$ is equal to zero for a pure state ρ_{AB} iff ρ_{AB} is not entangled, i.e. if it can be written as

$$\rho_{AB} = \rho_A \otimes \rho_B$$

and is smaller than zero for any entangled states.

14.5 Solve case (ii) of example 14.3 but for a symmetric channel where both qubits undergo amplitude damping[1] each with probability ℓ. This situation is realized if a central party Charlie produces the entangled state and distributes one qubit to Alice and the other to Bob.

14.6 When distributing photons the probability of a photon being lost goes exponentially with the distance L, i.e. $\ell = 1 - e^{-\gamma L}$. By comparing your results in exercise 14.3 with those in example 14.3 discuss which setup will be more suitable for the distribution of entangled pairs of photons.

[1] It may be helpful to assume that the two qubits may go through their channels in sequence when solving this problem.

15 Quantum Communication

Exercises

15.1 Consider a momentum entanglement interferometer experiment. Calculate the probability of coincidence clicks for all possible pairs of detectors assuming that the state

$$|\Psi\rangle = \frac{|ab\rangle + |ba\rangle}{\sqrt{2}} ,$$

is created in the down-conversion process as a function of the phase shift ϕ.

15.2 If down-conversion happened incoherently photon pairs in state

$$|\Psi\rangle = \frac{1}{\sqrt{2}} \left(e^{i\varphi} |ab\rangle + |ba\rangle \right)$$

would be generated with a phase φ that takes on any value $[0, 2\pi]$ with equal probability. Show that in this scenario the photon pairs are described by the density operator

$$\rho = \frac{1}{2} \left(|ab\rangle \langle ab| + |ba\rangle \langle ba| \right) .$$

15.3 Carry out the same calculation as in exercise 15.1 but now for the state generated in an incoherent process as in 15.2.

15.4 Using the symmetry properties of photons explain how the Bell states $|\Psi^{\pm}\rangle$ can be distinguished in a partial Bell state analyzer for polarization encoded photons. Why can the other two states not be distinguished? Imagine that photons were fermions (which is not true!). How would the partial Bell state analyzer work in this case?

15.5 For quantum dense coding Bob needs a Bell state analyzer. What is the channel capacity (number of classical bits transmitted in one use of the channel) if Bob has an ideal Bell state analyzer? How is this channel capacity reduced if the Bell state analyzer is only able to identify the two Bell states $|\Psi^{\pm}\rangle$ but cannot differentiate between the two Bell states $|\Phi^{\pm}\rangle$?

15.6 Work out descriptions of the quantum dense coding and teleportation protocols for the case where the EPR source produces the Bell state $|\Phi^{+}\rangle$.

15.7 Show that without classical communication no information about the state of qubit 1 is transferred to qubit 3 in the teleportation protocol. Explain why it is impossible to transmit the quantum state of a qubit from Alice to Bob by classical communication only.

15.8 Alice and Bob carry out the teleportation protocol with an imperfect Bell state analyzer which cannot distinguish the states $|\Phi^+\rangle$ and $|\Phi^-\rangle$. Assume that Alice does not tell Bob about this imperfection but randomly assumes one of the two states whenever the Bell state analyzer gives an ambiguous result. Calculate the fidelity with which an arbitrary state $|\psi\rangle$ is teleported in this case. Which states are teleported with maximum fidelity and which states are teleported with minimum fidelity?

15.9 Qubit 1 is entangled with a quantum system 4. Their state can be written as

$$|\Psi\rangle_{14} = \frac{|0\rangle_1 \otimes |\phi\rangle_4 + |1\rangle_1 \otimes |\varphi\rangle_4}{\sqrt{2}} .$$

Show that if the teleportation protocol is applied to qubit 1 the entanglement with system 4 is swapped to qubit 3. Does this protocol work if qubits 1 and 4 are initially in a mixed entangled state?

16 Testing EPR

Exercises

16.1 Work out the quantum mechanical expectation values for the combination of observables Q, R at Alice's site and S, T at Bob's site for the setup described in the Section on Aspect experiments. Show that they violate the CHSH inequality.

16.2 Derive a CHSH type inequality which is violated if the EPR source produces the state $|\Phi^-\rangle$.

16.3 In the ZZZ basis a GHZ state is given by

$$|\mathrm{GHZ}\rangle = \frac{1}{\sqrt{2}}(|HHH\rangle + |VVV\rangle)\,.$$

By rewriting this GHZ state in the bases XYY, YXY and YYX show that measuring two of the photons in circular polarization determines the polarization of the third photon in the X basis with certainty. Rewrite the GHZ state in the XXX basis and show that measuring in this XXX basis violates the expectations of local realism discussed in the lectures.

16.4 Calculate the probability with which the production of two photon pairs in the setup discussed in the lecture on GHZ states leads to a click in all four detectors and hence work out the fraction of events which must be disregarded at the post-selection stage assuming that a single down-conversion process happens with a probability of 10^{-3} for each light pulse entering the BBO crystal.

17 Quantum cryptography

Exercises

17.1 Assume that a communication channel used by Alice and Bob for BB84 key distribution is capable of transmitting 1000 qubits per second. What is the average key generation rate that Alice and Bob can achieve if they a) assume that no eavesdropper can be present and thus do not publicly compare parts of their key; b) an eavesdropper using intercept/resend strategy on each second qubit should be detected with 99.9% probability after two seconds. How much mutual information can be established between Alice's bit string A and the eavesdropper during these two seconds?

17.2 Calculate the joint probabilities $P_{ab}(\phi_A, \phi_B)$ introduced in example 17.1 explicitly and use them to work out $E(\phi_A, \phi_B)$). Show that your result is consistent with directly calculating $E(\phi_A, \phi_B) = \langle \Psi^- | \sigma_{\phi_A} \otimes \sigma_{\phi_B} | \Psi^- \rangle$.

17.3 Show how a difference in the optical path length of the two fibres connecting Alice and Bob in Figure 17.1(a) leads to errors in the BB84 protocol. Assume that this phase error is equally distributed in the interval $\Delta\phi \in [-\pi/20, \pi/20]$. What is the probability that Alice and Bob obtain different measurement outcomes when publicly comparing bits measured in the same basis?

17.4 For the phase encoding systems in Figure 17.1(b) determine the probability for a photon to be incident on B_1 and B_2 as a function of the two phases induced by the two independent phase modulators ϕ_A and ϕ_B. Note that for the setup shown in this figure the photons going along paths SS and LL are assumed not to contribute to the signal. Explain how this setups can be used to realize the BB84 protocol.