

Tutorials for Lectures 1, 2 and 3

Problems

Problem 1.1

Which of the following states are entangled? For those that are not entangled, give the decomposition as a product state. For simplicity of notation, we write $|\psi_1\rangle|\psi_2\rangle$ instead of $|\psi_1\rangle \otimes |\psi_2\rangle$.

1. $|\Psi_1\rangle = \cos \theta |0\rangle|0\rangle + \sin \theta |1\rangle|1\rangle$.
2. $|\Psi_2\rangle = \cos \theta |0\rangle|0\rangle + \sin \theta |1\rangle|0\rangle$.
3. $|\Psi_3\rangle = \frac{1}{2}(|0\rangle|0\rangle + |0\rangle|1\rangle - |1\rangle|0\rangle - |1\rangle|1\rangle)$.
4. $|\Psi_4\rangle = \frac{1}{2}(|0\rangle|0\rangle + |0\rangle|1\rangle + |1\rangle|0\rangle - |1\rangle|1\rangle)$.

Problem 1.2

Compute the partial states ρ_A and ρ_B for the following states of two qubits:

1. The pure state $|\Psi\rangle = \sqrt{\frac{2}{3}}|0\rangle|+\rangle + \sqrt{\frac{1}{3}}|+\rangle|-\rangle$; where $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$.
2. The mixed state $W(\lambda) = \lambda|\Psi^-\rangle\langle\Psi^-| + (1-\lambda)\frac{\mathbb{1}}{4}$, called Werner state [R.F. Werner, Phys. Rev. A **40**, 4277 (1989)].

Verify in both cases that ρ_A and ρ_B are mixed by computing the norm of their Bloch vectors.

Problem 1.3

This is a more advanced problem, inspired by: V. Scarani, M. Ziman, P. Štelmachovič, N. Gisin, V. Bužek, Phys. Rev. Lett. **88**, 090705 (2002).

We consider the following decoherent channel. A qubit, initially prepared in a state ρ , undergoes sequential “collisions” with qubits coming from a reservoir. All the qubits of the reservoir are supposed to be in state $\xi = p|0\rangle\langle 0| + (1-p)|1\rangle\langle 1|$. Each collision implements the evolution

$$U : \begin{cases} |0\rangle|0\rangle & \longrightarrow & |0\rangle|0\rangle \\ |0\rangle|1\rangle & \longrightarrow & \cos \phi |0\rangle|1\rangle + i \sin \phi |1\rangle|0\rangle \\ |1\rangle|0\rangle & \longrightarrow & \cos \phi |1\rangle|0\rangle + i \sin \phi |0\rangle|1\rangle \\ |1\rangle|1\rangle & \longrightarrow & |1\rangle|1\rangle \end{cases} \quad (1.3.1)$$

with $\sin \phi \neq 0$. We assume that each qubit of the reservoir interacts only once with the system qubit. Therefore, the state of the system after collision with $n + 1$ qubits of the bath is defined recursively as

$$\rho^{(n+1)} \equiv T_{\xi}^{n+1}[\rho] = \text{Tr}_B \left(U \rho^{(n)} \otimes \xi U^{\dagger} \right). \quad (1.3.2)$$

1. Let $\rho^{(n)} = d^{(n)}|0\rangle\langle 0| + (1 - d^{(n)})|1\rangle\langle 1| + k^{(n)}|0\rangle\langle 1| + k^{(n)*}|1\rangle\langle 0|$. Prove that the CP-map (1.3.2) induces the recursive relations

$$d^{(n+1)} = c^2 d^{(n)} + s^2 p, \quad k^{(n+1)} = c k^{(n)} \quad (1.3.3)$$

with $c = \cos \phi$ and $s = \sin \phi$.

2. By iteration, provide $d^{(n+1)}$ and $k^{(n+1)}$ as a function of the parameters of the initial state $d^{(0)}$ and $k^{(0)}$. Conclude that $T_{\xi}^n[\rho] \rightarrow \xi$ when $n \rightarrow \infty$, whatever the initial state ρ (pure or mixed).
3. We have just studied an example of “thermalization”: a system, put in contact with a large reservoir, ultimately assumes the same state as the particles in the reservoir. Naively, one would have described this process as $\rho \otimes \xi^{\otimes N} \rightarrow \xi^{\otimes N+1}$ for all ρ . Why is such a process not allowed by quantum physics?
4. The condition $\sin \phi \neq 0$ is necessary to have a non-trivial evolution during each collision; however, to have a meaningful model of thermalization one has to enforce $\cos \phi \gg |\sin \phi|$. What is the meaning of this condition? *Hint*: as a counter-example, consider the extreme case $\sin \phi = 1$: what is then U ? What does the process look like in this case?

Problem 2.1

Amplification of light is of course compatible with the no-cloning theorem, because spontaneous emission prevents amplification to be perfect [L. Mandel, Nature **304**, 188 (1983)]. Actually, if the amplifier is independent of the polarization, universal symmetric cloning of that degree of freedom is implemented [C. Simon, G. Weihs, A. Zeilinger, Phys. Rev. Lett **84**, 2993 (2000); J. Kempe, C. Simon, G. Weihs, Phys. Rev. A **62**, 032302 (2000)]. In this problem, we explore the basics of this correspondence.

Consider a single spatial mode of the electromagnetic field and focus on the polarization states; we denote by $|n, m\rangle$ the state in which n photons are polarized H and m photons are polarized V . Suppose one photon in mode H is initially present in the amplifier, and that after amplification 2 photons have been produced.

1. Compute the single-copy fidelity of this cloning process. *Hint*: if you don't remember the physics of amplification, you can reach the result by comparing $a_H^{\dagger}|1, 0\rangle$ with $a_V^{\dagger}|1, 0\rangle$.
2. How would you describe the state of the system (field + amplifier medium) in this process? *Hint*: compare with the B-H QCM.

Problem 3.1

Prove that the trace distance between two pure states $|\psi_1\rangle$ and $|\psi_2\rangle$ is given by

$$D(\rho_1, \rho_2) = \sqrt{1 - |\langle\psi_1|\psi_2\rangle|^2}. \quad (3.1.1)$$

Hint: Note that you can always find a basis in which $|\psi_1\rangle = c|0\rangle + s|1\rangle$ and $|\psi_2\rangle = e^{i\varphi}(c|0\rangle - s|1\rangle)$ with $c = \cos\theta$ and $s = \sin\theta$.

Problem 3.2

A short laser pulse can be sent either at time t_1 or at time t_2 . By detecting the time of arrival, one can obviously discriminate between these two cases. This rather trivial process is actually an example of *unambiguous state discrimination* of the two two-mode coherent states $|\psi_1\rangle = |0\rangle|\alpha\rangle$ and $|\psi_2\rangle = |\alpha\rangle|0\rangle$; it is used to create the raw key in the quantum cryptography protocol called COW [D. Stucki, N. Brunner, N. Gisin, V. Scarani, H. Zbinden, Appl. Phys. Lett. **87**, 194108 (2005)]. We recall the decomposition of the coherent state $|\alpha\rangle$, $\alpha \in \mathbb{C}$, on the number basis:

$$|\alpha\rangle = e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle. \quad (3.2.1)$$

1. What is the probability of success for optimal USD?
2. Prove that the POVM for optimal USD can simply be realized by detecting the time of arrival (with a perfect detector). *Hint:* What are the “inconclusive” events?
3. Discuss what happens if the detector is not perfect, in particular how the discussion is modified by (i) efficiency $\eta < 1$; (ii) dark counts.

Problem 3.3

Let $\{|e_k\rangle\}_{k=1\dots 4}$ be an orthonormal set of four vectors. We define $|\psi_1^\pm\rangle = \sqrt{1-\varepsilon}|e_1\rangle \pm \sqrt{\varepsilon}|e_2\rangle$ and $|\psi_2^\pm\rangle = \sqrt{1-\varepsilon}|e_3\rangle \pm \sqrt{\varepsilon}|e_4\rangle$; and we construct in turn the mixtures $\rho_0 = (1-\varepsilon)|\psi_1^+\rangle\langle\psi_1^+| + \varepsilon|\psi_2^+\rangle\langle\psi_2^+|$ and $\rho_1 = (1-\varepsilon)|\psi_1^-\rangle\langle\psi_1^-| + \varepsilon|\psi_2^-\rangle\langle\psi_2^-|$.

1. Compute the Holevo bound $\chi(\rho_0, \rho_1)$, assuming $p_0 = p_1 = \frac{1}{2}$.
2. The states given above, of course, have a meaning: they describe Eve’s states in the optimal eavesdropping on the BB84 protocol of quantum cryptography, when an error rate ε is measured by Alice and Bob (see other series of lectures; and V. Scarani et al., arXiv:0802.4155, in particular paragraph III.B.2 and Appendix A). In this scenario, what may the Holevo bound mean? *Hint:* the index a or the matrices ρ_a is Alice’s bit.

Tutorials for Lectures 1, 2 and 3

Solutions

Problem 1.1

$|\Psi_1\rangle$ is entangled.

$|\Psi_2\rangle = (\cos\theta|0\rangle + \sin\theta|1\rangle)|0\rangle$ is not entangled.

$|\Psi_3\rangle = \frac{1}{2}(|0\rangle - |1\rangle)(|0\rangle + |1\rangle) = |-\rangle|+\rangle$ is not entangled.

$|\Psi_4\rangle$ is entangled. This can be verified by direct calculation, or also by noticing that $|\Psi_4\rangle = \frac{1}{\sqrt{2}}(|0\rangle|+\rangle + |1\rangle|-\rangle)$; by just relabeling the basis of the second system, one sees that this state has the same form as $|\Psi_1\rangle$ with $\cos\theta = \sin\theta = \frac{1}{\sqrt{2}}$.

Problem 1.2

1. For the pure state under study, $\rho_A = \frac{2}{3}|0\rangle\langle 0| + \frac{1}{3}|+\rangle\langle +| = \frac{1}{2}(\mathbb{1} + \frac{2}{3}\sigma_z + \frac{1}{3}\sigma_x)$. In order to compute ρ_B , here is a possibility (maybe not the fastest one): first, rewrite the state as $|\Psi\rangle = |0\rangle\left(\sqrt{\frac{2}{3}}|+\rangle + \sqrt{\frac{1}{6}}|-\rangle\right) + \sqrt{\frac{1}{6}}|1\rangle|-\rangle$. Then

$$\begin{aligned}\rho_B &= \left(\sqrt{\frac{2}{3}}|+\rangle + \sqrt{\frac{1}{6}}|-\rangle\right)\left(\sqrt{\frac{2}{3}}\langle +| + \sqrt{\frac{1}{6}}\langle -|\right) + \frac{1}{6}|-\rangle\langle -| \\ &= \frac{2}{3}|+\rangle\langle +| + \frac{1}{3}|-\rangle\langle -| + \frac{1}{3}|+\rangle\langle -| + |-\rangle\langle +| = \frac{2}{3}|0\rangle\langle 0| + \frac{1}{3}|+\rangle\langle +| = \rho_A\end{aligned}$$

since $|0\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle)$. Note how, in this last calculation, the normalization is taken care of automatically.

The Bloch vector of $\rho_A = \rho_B$ has norm $|\vec{m}| = \frac{\sqrt{5}}{3} < 1$, therefore the states are mixed.

2. For the Werner state: $\rho_A = \rho_B = \frac{\mathbb{1}}{2}$. These states are maximally mixed, indeed $|\vec{m}| = 0$.

Problem 1.3

1. The first point is a matter of patience in writing down explicitly $U\rho^{(n)} \otimes \xi U^\dagger$, then noticing that $\text{Tr}(|0\rangle\langle 0|) = \text{Tr}(|1\rangle\langle 1|) = 1$ and $\text{Tr}(|0\rangle\langle 1|) = \text{Tr}(|1\rangle\langle 0|) = 0$.
2. For the off-diagonal term, the recursion is obviously

$$k^{(n+1)} = c^{n+1}k^{(0)}.$$

For the diagonal term, one has

$$\begin{aligned} d^{(n+1)} &= c^2 \left[c^2 d^{(n-1)} + s^2 p \right] + s^2 p = c^4 d^{(n-1)} + s^2(1+c^2)p = \dots \\ &= c^{2(n+1)} d^{(0)} + s^2 \sum_{k=0}^n c^{2k} p = c^{2(n+1)} d^{(0)} + [1 - c^{2(n+1)}]p \end{aligned}$$

because $\sum_{k=0}^n c^{2k} = \frac{1-c^{2(n+1)}}{1-c^2} = \frac{1-c^{2(n+1)}}{s^2}$. Therefore $d^{(n+1)} \rightarrow p$ and $k^{(n+1)} \rightarrow 0$ for $n \rightarrow \infty$.

3. The evolution $\rho \otimes \xi^{\otimes N} \rightarrow \xi^{\otimes N+1}$ is not unitary, since two initially different states would end up being the same.
4. For $\sin \phi = 1$, U is the swap operation. In this case, the ‘‘thermalization’’ would consist in dumping the initial system in the reservoir and replacing it with one of the qubits of the reservoir. Such a process would introduce a very large fluctuation in the reservoir. By setting $\cos \phi \approx 1$, on the contrary, one has $\text{Tr}(\rho_j A) \approx \text{Tr}(\xi A)$ for any qubit j , for any single-particle physical quantity A . In other words, the system *appears* to be completely thermalized and one has to measure some multi-particle physical quantities to see some differences. This view is perfectly consistent with the idea that irreversibility is only apparent.

Problem 2.1

1. The theory of spontaneous and stimulated emission implies that, starting with $|1, 0\rangle$, the probability of creating $|2, 0\rangle$ is twice as large as the probability of creating $|1, 1\rangle$. The single-copy fidelity is defined as the probability of finding one of the photons in the initial state, whence obviously $F = \frac{2}{3} \times 1 + \frac{1}{3} \times \frac{1}{2} = \frac{5}{6}$. This is identical to the fidelity for optimal universal symmetric cloning.
2. The analogy with cloning is actually exact: indeed, by conservation of angular momentum, the emission of an H photon and of a V photon cannot be due to the same process. Therefore, after amplification and post-selection of the emission of two photons, the state of the system ‘‘field + amplifying medium’’ reads $\sqrt{\frac{2}{3}}|2, 0\rangle \otimes |e_H\rangle + \sqrt{\frac{1}{3}}|1, 1\rangle \otimes |e_V\rangle$, i.e., in first-quantized notation

$$\sqrt{\frac{2}{3}}|H\rangle|H\rangle \otimes |e_H\rangle + \sqrt{\frac{1}{3}}|\Psi^+\rangle \otimes |e_V\rangle$$

and this exactly the state produced by the B-H QCM.

Problem 3.1

By writing $|\psi_1\rangle = c|0\rangle + s|1\rangle$ and $|\psi_2\rangle = e^{i\varphi}(c|0\rangle - s|1\rangle)$, we have $\langle\psi_1|\psi_2\rangle = e^{i\varphi}(c^2 - s^2) = e^{i\varphi} \cos 2\theta$ and

$$\rho_1 - \rho_2 = 2cs\sigma_x$$

whence $D(\rho_1, \rho_2) = \frac{1}{2}(|+2cs| + |-2cs|) = 2cs = \sin 2\theta$. The result follows immediately.

Problem 3.2

1. The probability of optimal USD is $p_{USD} = 1 - |\langle \psi_1 | \psi_2 \rangle|$; here $|\langle \psi_1 | \psi_2 \rangle| = |\langle 0 | \alpha \rangle|^2 = e^{-|\alpha|^2}$.
2. As soon as the detector fires, the two states can be distinguished; so the “inconclusive” events are the events in which the detector did not fire; if the detector has perfect efficiency, this can only happen because of the vacuum component of the state. In both $|\psi_1\rangle$ and $|\psi_2\rangle$, the amplitude of the vacuum component is $e^{-|\alpha|^2/2}$; therefore the probability that the detector fires is $1 - e^{-|\alpha|^2} = p_{USD}$.
3. A detector with efficiency $\eta < 1$ is equivalent to losses $\sqrt{\eta}$; the discrimination is still unambiguous but succeeds only with probability $p = 1 - e^{-\eta|\alpha|^2} < p_{USD}$ (note that this is still the optimal procedure, under the constraint that one has to use such imperfect detectors). If dark counts are present, the detector may fire even if there was no photon; therefore the discrimination is no longer unambiguous.

Problem 3.3

1. We have to compute $\chi(\rho_0, \rho_1) = S(\rho) - \frac{1}{2}[S(\rho_0) + S(\rho_1)]$ with $\rho = \frac{1}{2}(\rho_0 + \rho_1)$. Now, ρ_0 and ρ_1 are both incoherent mixtures of two orthogonal states with the same weights; therefore $S(\rho_0) = S(\rho_1) = -(1 - \varepsilon) \log(1 - \varepsilon) - \varepsilon \log \varepsilon \equiv h(\varepsilon)$. Moreover, $\rho = (1 - \varepsilon)^2 |e_1\rangle\langle e_1| + \varepsilon(1 - \varepsilon) |e_2\rangle\langle e_2| + \varepsilon(1 - \varepsilon) |e_3\rangle\langle e_3| + \varepsilon^2 |e_4\rangle\langle e_4|$, whence $S(\rho) = 2h(\varepsilon)$. All in all, $\chi(\rho_0, \rho_1) = h(\varepsilon)$.
2. One can see the relation between Alice and Eve as a channel, in which Alice’s bit value a has been encoded in a state ρ_a . Therefore, the Holevo bound represents the maximal information that Eve might extract about Alice’s bit.