Homework 6
Traitement Quantique de l'Information

Exercise 1 *Bell states*

The purpose of this exercise is to get you familiar with calculations involving Bell states: the calculations of the first three questions are in Dirac notation.

1) Show that the four Bell states introduced in class form an orthonormal basis of $\mathbb{C}^2 \otimes \mathbb{C}^2$.

2) Show that the state $|B_{00}\rangle$ (or take any other Bell states you like) is entangled. This means that there does not exist $|\phi_1\rangle, |\phi_2\rangle \in \mathbb{C}^2$ such that $|B_{00}\rangle = |\phi_1\rangle \otimes |\phi_2\rangle \in \mathbb{C}^2$.

3) Let $|\gamma\rangle = \cos\gamma\,|0\rangle + \sin\gamma\,|1\rangle$ and $|\gamma_\perp\rangle = -\sin\gamma\,|0\rangle + \cos\gamma\,|1\rangle$. Show the identity (for all angle of polarization γ)

$$|B_{00}\rangle = \frac{1}{\sqrt{2}}(|\gamma\rangle \otimes |\gamma\rangle + |\gamma_\perp\rangle \otimes |\gamma_\perp\rangle).$$

4) Represent the four Bell states in coordinates. Use the canonical representation $|0\rangle = (1,0)^\top$ and $|1\rangle = (0,1)^\top$.

Exercise 2 *Entanglement for two quantum bits*

Consider two quantum bits in the state:

$$|\Psi\rangle = \frac{1}{\sqrt{3}}\left(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle + i\,|1\rangle \otimes |0\rangle\right)$$

where $|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}$ and $|1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$ are the canonical orthonormal basis of $\mathbb{C}^2$.

1) Write this state in 4-component-form as a column vector (use the conventions of class for the tensor product).

2) Prove that this state is "entangled" (in french "intriquer") in the sense that *it is impossible to express it in "product form"*

$$(\alpha\,|0\rangle + \beta\,|1\rangle) \otimes (\gamma\,|0\rangle + \delta\,|1\rangle)$$

for any $\alpha, \beta, \gamma, \delta \in \mathbb{C}$.

Exercise 3 *Copying or unitary attack from Eve in BB84*

Consider the BB84 protocol. Suppose the i-th qubit sent by Alice is $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and is captured by Eve. Eve wants to make a copy of the qubit and sends one of the copies to Bob. However she does not know what the preparation basis of Alice was: here we suppose that Eve uses the wrong machine U_Z to copy this bit. Recall that U_Z is defined by

$$U_Z\,|0\rangle \otimes |b\rangle = |0\rangle \otimes |0\rangle\,, \quad U_Z\,|1\rangle \otimes |b\rangle = |1\rangle \otimes |1\rangle\,.$$

Eve then keeps one of the photons and sends the other one to Bob. Suppose now that Bob uses the X-basis to measure the state of the photon. During the public communication phase Alice and Bob notice that their preparation and measurement basis were the same so they conclude that the i-th bit (of their secret key) must be the same under the hypothesis that Eve is not present (they don't know yet that Eve is present).

The goal of this problem is to show that there is a probability $1/2$ that the bit of Alice and Bob differs due to the presence of Eve. Therefore repeated such attacks of Eve over many qubits will be detectable (with probability close to one) during the security test.

1) What is the state of the two photons in the lab of Eve just after she made the copying operation.

2) The measurement process of Bob (we suppose Eve does not measure at this stage) is modeled by the two projectors:

$$\Pi_+ = I \otimes \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{\langle 0| + \langle 1|}{\sqrt{2}}\right), \quad \Pi_- = I \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\left(\frac{\langle 0| - \langle 1|}{\sqrt{2}}\right)$$

where $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ expresses the fact that Eve does not measure and the second term of the tensor product expresses the fact that Bob's measurement basis is $\left\{ \frac{|0\rangle+|1\rangle}{\sqrt{2}}, \frac{|0\rangle-|1\rangle}{\sqrt{2}} \right\}$.

a) What are the possible resulting states in Bob's lab? Hint: no calculation.

b) Compute now $p_\pm$ the probability of these outcoming states by using the appropriate form of the measurement postulate.

Hint: It will be a good idea to expand $\Pi_\pm$ by writing $I = |0\rangle\langle 0| + |1\rangle\langle 1|$. For example you should check this kind of identity:

$$\begin{aligned}
\Pi_+ &= (|0\rangle\langle 0| + |1\rangle\langle 1|) \otimes \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{\langle 0| + \langle 1|}{\sqrt{2}}\right) \\
&= (|0\rangle\langle 0| + |1\rangle\langle 1|) \otimes \left(\frac{|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| + |1\rangle\langle 1|}{2}\right) \\
&= \frac{1}{2}\big(|00\rangle\langle 00| + |00\rangle\langle 01| + |01\rangle\langle 00| + |01\rangle\langle 01| \\
&\qquad + |10\rangle\langle 10| + |10\rangle\langle 11| + |11\rangle\langle 10| + |11\rangle\langle 11| \big)
\end{aligned}$$