Exercise sheet 2

Exercise 1. *Alice has a random bit $b \in \{0,1\}$ unknown to Bob. Consider the two following states*

$$|\psi_0\rangle = \sqrt{\frac{2}{3}}\,|00\rangle_{XY} + \sqrt{\frac{1}{3}}\,|11\rangle_{XY}$$
$$|\psi_1\rangle = \sqrt{\frac{1}{3}}\,|0+\rangle_{XY} + \sqrt{\frac{1}{3}}\,|1-\rangle_{XY} + \sqrt{\frac{1}{3}}\,|20\rangle_{XY}$$

1. *Assume Alice sends $\rho_b = Tr_X(|\psi_b\rangle\langle\psi_b|)$ to Bob. Show that this doesn't give him any information about b.*

2. *Assume Alice sends $|\psi_b\rangle$ to Bob. What is Bob's optimal probability of guessing b?*

Exercise 2. *We consider the following bit commitment between Alice and Bob, with a parameter α. In order to commit to a bit b, Alice chooses 2 random bits c_1, c_2 st. $c_1 \oplus c_2 = b$, creates*

$$\left|\psi^1_{A_1B_1}(c_1)\right\rangle = \sqrt{\alpha}\,|c_1\rangle\,|c_1\rangle + \sqrt{1-\alpha}\,|\overline{c_1}\rangle\,|\overline{c_1}\rangle$$
$$\left|\psi^2_{A_2B_2}(c_2)\right\rangle = \sqrt{\alpha}\,|c_2\rangle\,|c_2\rangle + \sqrt{1-\alpha}\,|\overline{c_2}\rangle\,|\overline{c_2}\rangle\,.$$

and sends registers B_1, B_2 to Bob. At the reveal phase, Alice reveals c_1, c_2, and the registers A_1, A_2. Bob checks that he has the state $\left|\psi^1_{A_1B_1}(c_1)\right\rangle$ in registers A_1, B_1 and the state $\left|\psi^2_{A_2B_2}(c_2)\right\rangle$ in registers A_2, B_2.

1. *Let $\rho_z = Tr_{A_1}|\psi^1_{A_1,B_1}(z)\rangle\langle\psi^1_{A_1,B_1}(z)| = Tr_{A_2}|\psi^2_{A_2,B_2}(z)\rangle\langle\psi^2_{A_2,B_2}(z)|$. Give the expression of ρ_0 and ρ_1 as a function of α.*

2. *Write a description of the following states: $\rho_0 \otimes \rho_0$, $\rho_0 \otimes \rho_1$, $\rho_1 \otimes \rho_0$, $\rho_1 \otimes \rho_1$.*

3. *Let ξ_b be the state that Bob receives from Alice after the commit phase. Show that*

$$\xi_0 = \frac{1}{2}(\alpha^2 + (1-\alpha)^2)\,(|00\rangle\langle 00| + |11\rangle\langle 11|) + (\alpha(1-\alpha))\,(|01\rangle\langle 01| + |10\rangle\langle 10|)$$
$$\xi_1 = \frac{1}{2}(\alpha^2 + (1-\alpha)^2)\,(|01\rangle\langle 01| + |10\rangle\langle 10|) + (\alpha(1-\alpha))\,(|00\rangle\langle 00| + |11\rangle\langle 11|)$$

4. *Assume Bob wants to guess b from ξ_b after the commit phase. What is his optimal probability P_B^* of guessing b? Give a measurement that achieves this optimal probability.*

5. *Recall that Alice's optimal cheating probability is $P_A^* = \frac{1}{2} + \frac{1}{2}F(\xi_0, \xi_1)$. Compute this cheating probability. For what value of α do we have $P_A^* = P_B^*$?*

6. *Find a strategy for Alice that allows her to reveal both $b = 0$ and $b = 1$, each with probability P_A^**