QII Exercise sheet 6

Exercise 1. *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*

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

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*

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

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*

Exercise 2 (Loss tolerant quantum coin flipping protocols with single qubits)**.** *We study the following generic bit commitment based quantum coin flipping scheme:*

Parameters : *two bipartite states $|\Phi^0_{AB}\rangle$ and $|\Phi^1_{AB}\rangle$. In particular we are interested in $\rho_0 = Tr_A(|\Phi^0_{AB}\rangle)$ and $\rho_1 = Tr_A(|\Phi^1_{AB}\rangle)$*

Protocol :

1. *Alice picks a random bit a, creates $|\Phi^a_{AB}\rangle$ and sends the B part to Bob.*
2. *Bob picks a random bit b and sends it to Alice.*
3. *Alice reveals her bit a and sends the second part of $|\Phi^a_{AB}\rangle$ to Bob. Bob checks that he has the correct state by projecting the state he has onto $|\Phi^a_{AB}\rangle$.*
4. *The outcome of the coin is $c = a \oplus b$.*

Cheating probabilities : *Here, cheating Alice's goal is to enforce outcome $c = 0$ while cheating Bob's goal is to enforce $c = 1$. We can use that the cheating probabilities for Alice and Bob can be written as*

$$P^*_A = \max \Pr[\textit{Alice cheats}] = \frac{1}{2} + \frac{F(\rho_0, \rho_1)}{2}$$
$$P^*_B = \max \Pr[\textit{Bob cheats}] = \frac{1}{2} + \frac{\Delta(\rho_0, \rho_1)}{2}$$

where F is the fidelity and Δ the trace distance. Recall that $F(\rho_0, \rho_1) = Tr(\sqrt{\sqrt{\rho_0}\sigma\sqrt{\rho_0}})$ and $\Delta(\rho_0, \rho_1) = \frac{1}{2}Tr(\sqrt{(\rho_0 - \rho_1)^2})$.

We also define P^*, the cheating probability of the protocol as $P^* = \max(P^*_A, P^*_B)$. Our goal is to study these protocols where the states ρ_a are single qubits.

1. *We add a parameter $x \in]0, 1[$ and consider a protocol with states $\rho_0 = |0\rangle\langle 0|$ and*
   $\rho_1 = (1-x)|0\rangle\langle 0| + x|1\rangle\langle 1|$. In this case, what are the cheating probabilities for Alice and Bob? Find x such that P^* is minimal. Show that this minimum P^* is equal to $\frac{1+\sqrt{5}}{4}$ (which is $\approx 81\%$).
2. *We now consider a parameter $x \in]1/2, 1[$ and a protocol with states $\rho_0 = x|0\rangle\langle 0| + (1-x)|1\rangle\langle 1|$ and $\rho_1 = (1-x)|0\rangle\langle 0| + x|1\rangle\langle 1|$. In this case, what are the cheating probabilities for Alice and Bob? Find x such that P^* is minimal. Show that this minimum P^* is equal to $\frac{1}{2} + \frac{\sqrt{2}}{4}$ (which is $\approx 85\%$).*

Losses: *We are now interested in the case where there are losses in the quantum channel. Losses imply that when Alice sends her qubit to Bob during step 1, he might not receive anything. If Bob didn't receive any qubit, he declares 'Loss' to Alice and they start again. Our goal is to see if a cheating Bob can use this to his advantage. A cheating Bob also has losses but when he actually receives the state ρ_a, he can still declare 'Loss' and start the protocol again.*

3. *We consider the first studied protocol with* $\rho_0 = |0\rangle\langle 0|$ *and* $\rho_1 = (1-x)|0\rangle\langle 0| + x|1\rangle\langle 1|$*, for any* $x \in]0,1[$*. Find a measurement* $\{|e_0\rangle, |e_1\rangle\}$ *for Bob with the following properties:*

   - $\Pr[$*Bob outputs* $|e_0\rangle$ $|$*Bob has* $\rho_0] = 1$
   - $\Pr[$*Bob outputs* $|e_0\rangle$ $|$*Bob has* $\rho_1] < 1$

   Use this measurement to describe (informally) a cheating strategy for Bob that works with probability 1 *in the presence of losses.*

4. *We consider the second studied protocol with* $\rho_0 = x|0\rangle\langle 0| + (1-x)|1\rangle\langle 1|$ *and* $\rho_1 = (1-x)|0\rangle\langle 0| + x|1\rangle\langle 1|$*, for any* $x \in]1/2,1[$*. Show that a measurement* $\{|e_0\rangle, |e_1\rangle\}$ *for Bob such that:*

   - $\Pr[$*Bob outputs* $|e_0\rangle$ $|$*Bob has* $\rho_0] = 1$
   - $\Pr[$*Bob outputs* $|e_0\rangle$ $|$*Bob has* $\rho_1] < 1$

   cannot exist.
   Conclusion: *This shows that even if the second protocol has a larger cheating probability, he cannot use the same strategy as in the for the previous protocol in order to cheat with probability* 1*.*

5. *Finally, we consider the protocol with* $\rho_0 = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|2\rangle\langle 2|$ *and* $\rho_1 = \frac{1}{2}|1\rangle\langle 1| + \frac{1}{2}|2\rangle\langle 2|$*. For this protocol, describe (informally) a cheating strategy that allows Bob to cheat with probability* 1 *in the presence of losses.*