

## QII Exercise sheet 14

**Exercise 1** (Quantum Weak Coin Flipping). *Alice and Bob interact and want to flip a random coin. Alice wins if they agree on outcome “0” and Bob wins on outcome “1”. Describe the construction seen in class (without looking at its description in the lecture notes) that shows how to use a bit commitment protocol with cheating probabilities  $P_A^*$ ,  $P_B^*$  to perform a coin flipping protocol with the same winning probabilities. Hint: consider a protocol where Alice commits to a bit  $b$ , receives a message from Bob and then reveals  $b$ .*

**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  $|\Phi_{AB}^0\rangle$  and  $|\Phi_{AB}^1\rangle$ . In particular we are interested in  $\rho_0 = \text{Tr}_A(|\Phi_{AB}^0\rangle)$  and  $\rho_1 = \text{Tr}_A(|\Phi_{AB}^1\rangle)$*

**Protocol :**

1. *Alice picks a random bit  $a$ , creates  $|\Phi_{AB}^a\rangle$  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  $|\Phi_{AB}^a\rangle$  to Bob. Bob checks that he has the correct state by projecting the state he has onto  $|\Phi_{AB}^a\rangle$ .*
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*

$$P_A^* = \max \Pr[\text{Alice cheats}] = \frac{1}{2} + \frac{F(\rho_0, \rho_1)}{2}$$

$$P_B^* = \max \Pr[\text{Bob cheats}] = \frac{1}{2} + \frac{\Delta(\rho_0, \rho_1)}{2}$$

*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  $\rho_a$  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  $\rho_a$ , 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:
  - $\Pr[\text{Bob outputs } |e_0\rangle \mid \text{Bob has } \rho_0] = 1$
  - $\Pr[\text{Bob outputs } |e_0\rangle \mid \text{Bob has } \rho_1] < 1$

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:
  - $\Pr[\text{Bob outputs } |e_0\rangle \mid \text{Bob has } \rho_0] = 1$
  - $\Pr[\text{Bob outputs } |e_0\rangle \mid \text{Bob has } \rho_1] < 1$

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.

**Exercise 3.** Our goal is to show the following result given in class: for any quantum states  $\rho, \sigma$ , we have

$$\max_{\zeta} \left\{ \frac{1}{2} F^2(\rho, \zeta) + \frac{1}{2} F^2(\zeta, \sigma) \right\} = \frac{1}{2} + \frac{F(\rho, \sigma)}{2}. \quad (1)$$

1. Show that for any angles  $\alpha, \beta \in [0, \pi/2]$

$$\cos(\alpha + \beta) \geq \cos^2(\alpha) + \cos^2(\beta) - 1.$$

(Hint: you can use the following inequality that comes from the concavity of the cos function on  $[0, \pi]$ :

$$\forall x, y \in [0, \pi] : \cos\left(\frac{x+y}{2}\right) \geq \frac{1}{2} (\cos(x) + \cos(y)).$$

as well as known trigonometric equalities)

2. Using the angle distance, show that

$$\max_{\zeta} \left\{ \frac{1}{2} F^2(\rho, \zeta) + \frac{1}{2} F^2(\zeta, \sigma) \right\} \leq \frac{1}{2} + \frac{F(\rho, \sigma)}{2}.$$

3. For any states  $\rho, \sigma$ , show that there exists  $\zeta$  st.

$$\frac{1}{2} F^2(\rho, \zeta) + \frac{1}{2} F^2(\zeta, \sigma) \geq \frac{1}{2} + \frac{F(\rho, \sigma)}{2}.$$

(Hint: Consider purifications  $|A\rangle, |B\rangle$  of  $\rho, \sigma$  from Uhlmann's theorem and look at the state "in between"  $|A\rangle$  and  $|B\rangle$ .)