## QII Exercise sheet 11-12

**Notations.** $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Trignometric relations:

$$\cos(x+y) = \cos(x)\cos(y) - \sin(x)\sin(y)$$
$$\sin(x+y) = \sin(x)\cos(y) + \sin(y)\cos(x)$$

In particular: $\cos(2x) = 2\cos^2(x) - 1$ and $\sin(2x) = 2\cos(x)\sin(x)$.
We define

$$Angle(\rho, \sigma) = arccos(F(\rho, \sigma)).$$

which implies that $Angle(\rho, \sigma) \in [0, \pi/2]$ and $F(\rho, \sigma) = \cos(Angle(\rho, \sigma))$. The angle is a distance measure and satisfies in particular the triangle inequality for any $\rho, \zeta, \sigma$:

$$Angle(\rho, \zeta) \leq Angle(\rho, \sigma) + Angle(\sigma, \zeta).$$

**Exercise 1.** *Our goal is to show the following result given in class: for any quantum states $\rho, \sigma$, we have*

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

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 $[0, \pi]$:*

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

*as well as known trigonometric equalities)*

2. *Using the angle distance, show that*

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

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 Ulhmann's theorem and look at the state " in between" $|A\rangle$ and $|B\rangle$.)*

# Analysis around the fingerprint state

Consider the state

$$|\psi_{x_1x_2x_3x_4}\rangle = \frac{1}{2}\left((-1)^{x_1}|00\rangle + (-1)^{x_2}|01\rangle + (-1)^{x_3}|10\rangle + (-1)^{x_4}|11\rangle\right).$$

that depends on 4 bits $x_1, x_2, x_3, x_4$.

**Exercise 2.** *We assume $x_2, x_3, x_4 = 0$. Consider the states $|\phi_b\rangle$ from the previous section. This is 2-qubit state on some registers $AB$ where $A$ is the register corresponding to the first qubit and $B$ is the register corresponding to the second qubit.*

1. *Compute $\rho_b^A = tr_B|\phi_b\rangle\langle\phi_b|$ for both $b = 0$ and $b = 1$.*
2. *Compute $\Delta(\rho_0^A, \rho_1^A)$. Give a measurement that, given $\rho_b^A$, outputs $b$ with probability $P_b$ with $\frac{1}{2}(P_0 + P_1) = \frac{3}{4}$ and argue that this measurement is optimal.*

**Exercise 3.** *We still assume $x_2, x_3, x_4 = 0$. Our goal is to analyze what is the probability of recovering $x_1$ from $|\psi_{x_1000}\rangle$.*

1. *Give an expression for $|\phi_0\rangle = |\psi_{0000}\rangle$ and $|\phi_1\rangle = |\psi_{1000}\rangle$.*
2. *Compute $\langle\phi_0|\phi_1\rangle$. Argue that there is a measurement that, given $|\phi_b\rangle$ for $b \in \{0, 1\}$, outputs $b$ with probability $P_b$ with $\frac{1}{2}(P_0 + P_1) = \frac{1}{2} + \frac{\sqrt{3}}{4}$.*
3. *Find the measurement that distinguishes $|\phi_0\rangle$ and $|\phi_1\rangle$ wp. $\frac{1}{2} + \frac{\sqrt{3}}{4}$. One can use without proof $\frac{1}{2} + \frac{\sqrt{3}}{4} = \cos^2(\pi/12)$.*

**Exercise 4.** *We now don't have $x_2, x_3, x_4 = 0$ anymore. Assume we are in one of the two following cases*

1. *$x_1 = x_2 = x_3 = x_4$.*
2. *$x_1 \oplus x_2 \oplus x_3 \oplus x_4 = 0$, but the 4 bits are not all equal.*

*Give a measurement on $|\psi_{x_1x_2x_3x_4}\rangle$ that determines with certainty in which case we are.*

**Exercise 5** (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". Show (without looking at the lecture notes) how to use a bit commitment protocol with cheating probabilites $P_A^*, P_B^*$ 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 6** (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 $\Delta$ 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 $\rho_a$ 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:*

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

   *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.*