Practice problem set 8

You do not have to hand in these exercises, they are for practicing only.

Problem 1: Rabin OT vs 1-2 OT

Show how to obtain Rabin Oblivious Transfer when given 1-2 OT and vice versa.

Problem 2: A Simple Quantum Bit Commitment Protocol, Problem 2 of Chapter 8

(a) As you know very well by now, perfectly secure quantum bit commitment is impossible. Nonetheless, it is possible to construct protocols in which Alice and Bob can cheat to some extent, but not completely.

For a cheating Alice and honest Bob, we define Alice's cheating probability as $P_A = \frac{1}{2}(\Pr[\text{Alice opens } b=0 \text{ successfully}] + \Pr[\text{Alice opens } b=1 \text{ successfully}])$, maximized over Alice's (cheating) strategies. For a cheating Bob and an honest Alice, instead, we let Bob's cheating probability be $P_B = \Pr[\text{Bob guesses } b \text{ after the commit phase}]$, maximized over Bob's (cheating) strategies. The cheating probability of the protocol as a whole is then defined as $\max\{P_A, P_B\}$. In this question, we introduce a simple example of such a protocol:

In the *commit phase*, Alice commits to bit b by preparing the state $|\psi_b\rangle = \sqrt{\alpha}|bb\rangle + \sqrt{1-\alpha}|22\rangle$, and sending the second qutrit to Bob. In the *open phase*, she reveals the classical bit b and sends the first qutrit over to Bob, who checks that the pure state is the correct one, by making a measurement with respect to any orthogonal basis containing $|\psi_b\rangle$.

What is the density matrix ρ_b that Bob has after the commit phase if Alice has commited to bit b and honestly prepared state $|\psi_b\rangle$?

(b) Compute Bob's cheating probability P_B by recalling the operational interpretation of trace distance.

(c) Next, let's calculate Alice's cheating probability. Let the underlying Hilbert space be $\mathcal{H} \otimes \mathcal{H}_s \otimes \mathcal{H}_t$, where $\mathcal{H}_t$ corresponds to the qutrit that is sent to Bob in the commit phase, $\mathcal{H}_s$ to the qutrit that is sent during the opening phase, and $\mathcal{H}$ is any auxiliary system that Alice might use. For the most general strategy, we can assume that she prepares the pure state $|\phi\rangle$, as it can always be purified on $\mathcal{H}$. We can write $|\phi\rangle = \sum_i \sqrt{p_i}|i\rangle|\tilde{\psi}_{i,b}\rangle$ where $\{|i\rangle\}$ and $\{|\tilde{\psi}_{i,b}\rangle\}$ are Schmidt bases of $\mathcal{H}$ and $\mathcal{H}_s \otimes \mathcal{H}_t$ respectively. So, the reduced density matrix on $\mathcal{H}_s \otimes \mathcal{H}_t$ is $\sigma_b = \sum_i p_i |\tilde{\psi}_{i,b}\rangle\langle\tilde{\psi}_{i,b}|$. Moreover, let σ be Bob's reduced density matrix after the commit phase, i.e. just a qutrit. Now, compute the probability of dishonest Alice successfully opening bit b in terms of the fidelity of two density matrices, and hence give the following upper bound on Alice's cheating probability:

$$P_A^* \leq \frac{1}{2}\left(F(\sigma, \rho_0) + F(\sigma, \rho_1)\right)$$

Hint: use the fact that the fidelity is non-decreasing under taking partial trace, in particular tracing out system $\mathcal{H}_s$.

(d) Remember the property of fidelity that for any three density matrices ρ_1, ρ_2, ρ_3, it holds that $F^2(\rho_1, \rho_2) + F^2(\rho_1, \rho_3) \leq 1 + F(\rho_2, \rho_3)$. Give an upper bound to Alice's cheating probability in terms of α

(e) Note that the bound on Bob's cheating probability that you obtained in Problem b is tight, since it is the best possible probability of distinguishing between two known states, and he knows what the two states are when Alice is honest.

Importantly, the bound above on Alice's cheating probability that we just obtained is also tight. There is a simple cheating strategy that allows Alice to achieve this bound, without even making use of the auxiliary system $\mathcal{H}$. What state(s) of two qutrits can she prepare?

(f) Finally, by combining the calculations so far on Alice and Bob's cheating probabilities, determine the α that minimizes the overall cheating probability of the protocol. What is the overall cheating probability?

Problem 3: A Weak Coin-Flipping Protocol (Problem 1 of Chapter 8)

In these week's lectures, you have been presented with an example of a strong quantum coin flipping protocol with bias $1/4$. In this prob-

lem you'll see how a variation of that same protocol allows to construct a weak coin flipping protocol with bias smaller than $1/4$. This is still far from the best weak coin flipping protocol that we know of (in fact weak coin flipping protocols exist with arbitrarily small bias), but it is still instructive to consider, and to go through its security. Recall that in a weak coin flipping protocol, one of the outcomes is identified with "Alice wins" and the other with "Bob wins", so each player hopes for just one of the two outcomes. In this context, for a cheating Alice and honest Bob, we define Alice's cheating probability as $P_A^* = \Pr[\text{Alice wins}]$, maximized over Alice's (cheating) strategies, and similarly P_B for Bob, and we say that the cheating probability of the protocol is $\max\{P_A, P_B\}$. The protocol in this problem is parametrised by $\alpha \in [0, \pi]$, over which you'll optimise later on. We use the term "qutrit" to refer to a quantum state in the space $\mathbb{C}^3$, i.e. a state of the form $\alpha_0|0\rangle + \alpha_1|1\rangle + \alpha_2|2\rangle$. For $a, x \in \{0, 1\}$, define the qutrit state $|\psi_{a,x}\rangle$ in the space $\mathcal{H}_t = \mathbb{C}^3$ as

$$|\psi_{a,x}\rangle = \cos(\frac{\alpha}{2})|0\rangle + \sin(\frac{\alpha}{2})(-1)^x|a+1\rangle$$

and $|\psi_a\rangle \in \mathcal{H}_s \otimes \mathcal{H}_t = \mathbb{C}^2 \otimes \mathbb{C}^3$ as

$$|\psi_a\rangle = \frac{1}{\sqrt{2}}(|0\rangle|\psi_{a,0}\rangle + |1\rangle|\psi_{a,1}\rangle)\,.$$

The protocol runs as follows:

1. Alice picks $a \in_R \{0, 1\}$, prepares the state $|\psi_a\rangle \in \mathcal{H}_s \otimes \mathcal{H}_t$ (i.e. a state of one qubit and one qutrit) and sends to Bob the right half of the state (the qutrit).

2. Bob picks $b \in_R \{0, 1\}$ and sends it to Alice.

3. Alice then reveals the bit a to Bob. Let $c = a \oplus b$. If $c = 0$, then Alice sets $c_A = 0$ and sends to Bob the other part of the state $|\psi_a\rangle$ (the qubit). Bob checks that the qutrit-qubit pair he received is indeed in the state $|\psi_a\rangle$ (by taking a measurement with respect to any orthogonal basis of $\mathcal{H}_s \otimes \mathcal{H}_t$ containing $|\psi_a\rangle$). If the test is passed, Bob sets $c_b = 0$, and so Alice wins, else Bob concludes that Alice has deviated from the protocol, and aborts.

4. If, on the other hand, $c = a \oplus b = 1$, then Bob sets $c_B = 1$, and returns the qutrit he received in round 1. Alice checks that her qubit-qutrit pair is in state $|\psi_a\rangle$. If the test is passed, she sets $c_A = 1$ so Bob wins the game, else Alice concludes that Bob has tampered with her qutrit to bias the game, and aborts.

It is clear that if both players are honest, then the protocol is fair. We'll analyse what happens when one of the players cheats and the other is honest.

(a) What is Bob's reduced density matrix ρ_a after step 1, in the case that Alice has prepared the honest state $|\psi_a\rangle$? (note that the subscript a refers to the classical bit and not the system of Alice or Bob.)

(b) Now, suppose Bob is honest and Alice potentially cheats. We intend to obtain a (tight) bound on Alice's winning probability. The most general strategy is for Alice to prepare a pure state $|\phi\rangle \in \mathcal{H} \otimes \mathcal{H}_s \otimes \mathcal{H}_t$ where $\mathcal{H}$ is an auxiliary space (one can always purify the state via $\mathcal{H}$). Then she sends the qutrit part in $\mathcal{H}_t$ to Bob, and keeps the part of the state in $\mathcal{H} \otimes \mathcal{H}_s$. We can assume without loss of generality that in step 3 of the protocol Alice always replies with $a = b$ (so that $c = 0$), and consequently tries to pass Bob's check. For this, she performs a unitary U_b on her part of $|\phi\rangle$, so that she gets $|\phi_b\rangle = (U_b \otimes I)|\phi\rangle$, and then sends the qubit in $\mathcal{H}_s$ to Bob. The final joint state can then be written as $|\phi_b\rangle = \sum_i \sqrt{p_i}|i\rangle|\phi_{i,b}\rangle$ for some p_i's and Schmidt bases $\{|i\rangle\}$ of $\mathcal{H}$ and $\{|\phi_{i,b}\rangle\}$ of $\mathcal{H}_s \otimes \mathcal{H}_t$.

Now, recall the interpretation of the fidelity between to density matrices as the square root of the probability that Alice can convince Bob that one is the other. Let σ_b be the density matrix of Bob's qubit-qutrit pair at the end of the protocol. And let σ be Bob's reduced density matrix after the first step of the protocol (i.e. just the qutrit).

Prove the following upper bound on the probability that Alice wins given that Bob sent b:

$$\Pr[\text{Alice wins} \mid \text{Bob sent } b] \leq F^2(\sigma, \rho_b)\,.$$

Hint: express it first in terms of the fidelity of two density matrices and then use the fact that fidelity is non-decreasing under taking partial trace.

(c) Remember the property of fidelity that for any three density matrices σ, ρ_0, ρ_1, it holds that $F^2(\sigma, \rho_0) + F^2(\sigma, \rho_1) \leq 1 + F(\rho_0, \rho_1)$ Use this fact to upper-bound the probability that Alice wins in terms of α.

(d) Now, we turn to Bob's winning probability when he is potentially cheating and Alice is honest. He will be trying to infer as much as he can about the value of the bit a, so that he can send back a bit b such that $a \oplus b = 1$, at the same time trying to cause as little disturbance as possible to the joint state $|\psi_a\rangle$, so as to pass Alice's final check.

The most general strategy that he can employ is to perform a unitary U on the space $\mathcal{H}_t \otimes \mathcal{H} \otimes \mathbb{C}^2$ of the qutrit he received from Alice in $\mathcal{H}_t$, some auxiliary qubits in $\mathcal{H}$ and a qubit reserved for his reply. He then measures the last qubit and sends the outcome as b to Alice. Suppose without loss of generality that the unitary is such that

$$U : |i\rangle|\overline{0}\rangle|0\rangle \mapsto |\xi_{i,0}\rangle|0\rangle + |\xi_{i,1}\rangle|1\rangle$$

where $|\overline{0}\rangle$ is the initial state of the auxiliary qubits, and for some states $|\xi_{i,0}\rangle, |\xi_{i,1}\rangle$, not necessarily orthogonal, such that $\||\xi_{i,0}\rangle\|^2 + \||\xi_{i,1}\rangle\|^2 = 1$.

Show the following upper bound for the probability that Bob wins given that Alice sent a:

$$\begin{aligned}&\Pr[\text{Bob wins} \mid \text{Alice picked } a] \\ &\leq \left|\cos^2(\frac{\alpha}{2})(\langle 0| \otimes \mathbb{1})|\xi_{0,\overline{a}}\rangle + \sin^2(\frac{\alpha}{2})(\langle a+1| \otimes \mathbb{1})|\xi_{a+1,\overline{a}}\rangle\right|^2\end{aligned}$$

(e) Use the above to conclude that

$$\Pr[\text{Bob wins} \mid \text{Alice picked } a] \leq \left(\cos^2(\frac{\alpha}{2})\||\xi_{0,\overline{a}}\rangle\| + \sin^2(\frac{\alpha}{2})\right)^2 .$$

(f) Maximize over the choice of $|\xi_{0,0}\rangle$ and $|\xi_{0,1}\rangle$ to obtain that

$$\Pr[\text{Bob wins}] \leq \left(\frac{1}{\sqrt{2}}\cos^2(\frac{\alpha}{2}) + \sin^2(\frac{\alpha}{2})\right)^2 .$$

(g) Now, you may assume that the upper bounds you found for Alice and Bob's winning probabilities are both tight, i.e. there's a cheating strategy for each of Alice and Bob that achieves those bounds.

Determine the value of the parameter α that minimizes the overall bias of the protocol. What is the bias?