Assignment—Part II

Due at 23:59 on Friday, August whatever, 2014.

Typeset solutions can be e-mailed to the instructor. Alternately, hard copies can be placed in the instructor's mailbox in the QNC building.

In this assignment we derive a lower bound on the probability with which one of the parties can successfully cheat in any protocol for quantum bit commitment.

Recall the notation from lecture: $\mathcal{A}, \mathcal{B}$ denote the Hilbert spaces for the local registers of Alice, Bob. Suppose honest-Alice wishes to commit bit $b \in \{0,1\}$ and let $|\psi_b\rangle \in \mathcal{A} \otimes \mathcal{B}$ denote the pure state of the entire system at the end of the commit phase when both parties are honest. Let $\rho_b = \mathrm{Tr}_{\mathcal{A}}(|\psi_b\rangle\langle\psi_b|)$ denote the reduced state of Bob's local portion of the system. For simplicity we assume that honest-Alice chooses her bit b uniformly at random at the beginning of the protocol.

The goal of cheating-Bob is to guess honest-Alice's bit b after the commit phase but before the reveal phase. We define the quantity

$$p_{\text{Bob}} = \Pr[\text{cheating-Bob guesses } b \text{ before the reveal phase}]$$

and observe that $p_{\text{Bob}} \geq 1/2$ in any protocol for quantum bit commitment because a random guess is correct with probability $1/2$.

The goal of cheating-Alice is to be able to reveal any value $b \in \{0,1\}$ chosen *after* the commit phase. The extent to which she can achieve this goal is quantified by the average of the two probabilities with which she can successfully reveal the two different possible values of b:

$$p_{\text{Alice}} = \frac{1}{2}\left(\Pr[\text{cheating-Alice sucessfully reveals } b = 0] + \Pr[\text{cheating-Alice sucessfully reveals } b = 1]\right).$$

Observe that $p_{\text{Alice}} \geq 1/2$ in any protocol for quantum bit commitment because cheating-Alice can act honestly to reveal one of the two values $b \in \{0,1\}$ with certainty.

In this assignment we will prove that $\max\{p_{\text{Alice}}, p_{\text{Bob}}\} \geq 63\%$ in any protocol for quantum bit commitment.

We begin by specifying cheating strategies for both Alice and Bob in any protocol. Our cheating-Bob acts honestly during the commit phase. Once the commit phase is complete, our cheating-Bob performs a measurement to try to guess b.

Because our cheating-Bob acts honestly during the commit phase, he holds ρ_b after the commit phase. Because b was chosen by honest-Alice uniformly at random, cheating-Bob is faced with a simple state discrimination problem in which he is asked to identify a state sampled uniformly at random from $\{\rho_0, \rho_1\}$. It is widely known that the maximum probability with which Bob can successfully guess b in this scenario is

$$p_{\text{Bob}} = \frac{1}{2} + \frac{1}{4}\|\rho_0 - \rho_1\|_{\text{Tr}}.$$

I will not ask you to prove this fact, but it is a fundamental fact worth knowing so I suggest you look it up.

Our cheating-Alice acts honestly during the commit phase in order to commit to $b = 0$. If cheating-Alice is asked to reveal 0 then she completes the protocol honestly as though revealing 0. If cheating-Alice is asked to reveal 1 then she applies a unitary U specified below to her portion of the system and then completes the protocol honestly as though revealing 1.

For our cheating-Alice it is clear that

$$\Pr[\text{cheating-Alice sucessfully reveals } b = 0] = 1$$

since in this case cheating-Alice acts honestly throughout the entire protocol to reveal $b = 0$. One of our goals in this assignment is to bound the other probability

$$\Pr[\text{cheating-Alice sucessfully reveals } b = 1]$$

in terms of $\| \rho_0 - \rho_1 \|_{\mathrm{Tr}}$—the quantity that dictates cheating-Bob's success probability p_{Bob}.

To this end we view the reveal phase of the protocol as a three-outcome POVM measurement $\{P_0, P_1, P_{\text{abort}}\}$ jointly implemented by cheating-Alice and honest-Bob in which outcome $c \in \{0, 1\}$ indicates that cheating-Alice has successfully revealed bit $b = c$ to honest-Bob and outcome 'abort' indicates that honest-Bob has caught Alice cheating. Because cheating-Alice acts honestly to reveal 1, it must be that

$$\mathrm{Tr}(P_1 |\psi_1\rangle\langle\psi_1|) = 1.$$

However, the state to which this measurement is actually applied is not $|\psi_1\rangle$ but is instead

$$|\psi'\rangle \stackrel{\text{def}}{=} (U \otimes I_{\mathcal{B}})|\psi_0\rangle.$$

In other words,

$$\Pr[\text{cheating-Alice sucessfully reveals } b = 1] = \mathrm{Tr}\left(P_1 |\psi'\rangle\langle\psi'|\right).$$

Intuitively, this probability should depend upon the observable difference between $|\psi_1\rangle$ and $|\psi'\rangle$. You will now formalize this idea.

1. **Close states produce similar measurement results.** *[5 marks.]* Let ρ, ξ be mixed quantum states and let $\{P_0, P_1\}$ be a POVM measurement, meaning that $P_0, P_1 \succeq 0$ and $P_0 + P_1 = I$. Suppose that $\| \rho - \xi \|_{\mathrm{Tr}} \leq \delta$ and suppose that the measurement $\{P_0, P_1\}$ yields outcome 1 with certainty when applied to a system in state ρ.

   Prove that the probability with which $\{P_0, P_1\}$ yields outcome 1 when applied to a system in state ξ is at least $1 - \delta/2$.

   Hint: Use the fact that $\| \rho - \xi \|_{\mathrm{Tr}} = 2 \max_{0 \preceq P \preceq I} \mathrm{Tr}(P(\rho - \xi))$ for every choice of states ρ, ξ.

Thus, if $|\psi'\rangle$ is δ-close in trace distance to $|\psi_1\rangle$ then cheating-Alice should be able to reveal $b = 1$ with probability at least $1 - \delta/2$. Let us now derive a bound on δ.

Uhlmann's Theorem states that for any two mixed quantum states ρ, ξ on a space $\mathcal{B}$ and any two purifications $|\phi\rangle, |\psi\rangle \in \mathcal{A}\mathcal{B}$ of ρ, ξ the fidelity $F(\rho, \xi)$ is given by

$$F(\rho, \xi) = \max_{U} |\langle\phi|(U \otimes I_{\mathcal{B}})|\psi\rangle|$$

where the maximization is over all unitary operators U acting on $\mathcal{A}$.

The aforementioned unitary U applied by our cheating-Alice is the unitary achieving the above maximum for $F(\rho_0, \rho_1)$ with purifications $|\psi_0\rangle, |\psi_1\rangle$.

2. **If Bob cannot cheat then Alice can.** *[5 marks.]* Write $\varepsilon = \|\rho_0 - \rho_1\|_{\mathrm{Tr}}$ so that $p_{\mathrm{Bob}} = \frac{1}{2} + \frac{1}{4}\varepsilon$.

   Prove that

   $$\Pr[\text{cheating-Alice sucessfully reveals } b = 1] \geq 1 - \sqrt{\varepsilon},$$

   from which it follows that $p_{\mathrm{Alice}} \geq 1 - \frac{1}{2}\sqrt{\varepsilon}$.

   Hint: First use question 1 to bound this probability in terms of the trace distance between $|\psi_1\rangle$ and $|\psi'\rangle$. Then use the following equality relating the trace distance between two pure states $|\psi_1\rangle, |\psi'\rangle$ to their inner product:

   $$|\langle\psi_1|\psi'\rangle|^2 = 1 - \frac{1}{4}\left\||\psi_1\rangle\langle\psi_1| - |\psi'\rangle\langle\psi'|\right\|_{\mathrm{Tr}}^2.$$

   Then use Uhlmann's Theorem to relate the inner product $|\langle\psi_1|\psi'\rangle|$ to the fidelity $F(\rho_0, \rho_1)$. Finally, use the following inequality relating the trace distance to the fidelity:

   $$1 - \frac{1}{2}\|\rho_0 - \rho_1\|_{\mathrm{Tr}} \leq F(\rho_0, \rho_1).$$

3. **Unconditionally secure quantum bit commitment is impossible.** *[5 marks.]* Use question 2 to prove that in any quantum bit commitment protocol it must be that $\max\{p_{\mathrm{Alice}}, p_{\mathrm{Bob}}\} \geq 0.63$.

   Hint: You can use software to solve a quadratic equation.