CS/Ph120 Homework 8 Solutions

December 2, 2016

Problem 1: Thinking adversarially.

Solution: (Due to De Huang)

- Attack to portocol 1:
  - Assume that Eve has a quantum machine that can store arbitrary amount of quantum states.
  - After Alice sends out the qubits she prepares via the quantum channel, Eve captures and stores them for the moment.
  - When Alice announces the basis string θ via the authenticated channel, Eves learns the basis. So Eve can measure the qubits in the right basis to learn the key x exactly without changing the qubits.
  - Afterwards Eve sends the unchanged qubits to Bob.
  - Since Bob receives the exact qubits that Alice sneds at the beginning and measures them in the right basis, the x they share will pass the correctness checking.
- Protocol improvement: Bob announces reception when he receives Alice's qubits. Alice announces the basis string θ only after Bob announces reception.
- Attack to protocol 2:
  - Assume that Eve has a quantum machine that can store and generate arbitrary amount of quantum states.
  - After Alice sends out the n halves of her EPR pairs via the quantum channel, Eve captures and stores them. (They become AE pairs.)
  - Eve generate another n EPR pairs and sends one half of each to Bob to cheat Bob, so that Bob will announce reception. (They become EB pairs.)
  - After Alice and Bob announce their basis strings θ and $\hat{\theta}$, Eve uses these bases to measure the qubits on her side(of AE pairs and of EB pairs repectively), and learns exactly the raw key x shared with Alice and the raw key $\hat{x}$ shared with Bob.
  - Eve only keeps the bits x_i and $\hat{x}_i$ for i such that $\theta_i = \hat{\theta}_i$. Now Eve has the exact key x that Alice will use and the exact key $\hat{x}$ that Bob will use.

- Protocol improvement: Alice and Bob carry out an additional correctness checking step before they use the keys x and $\hat{x}$ as a common key. (Under such attack, the final keys x and $\hat{x}$, whose expected lengths are $\frac{n}{2}$, are expected to share only $\frac{n}{4}$ matching bits.)

Problem 2: BB84 fails in the device-independent setting.

Solution: (Due to Mandy Huo)

(a) In this case the box measures the first qubit in the standard basis so the first qubit of Alice's state is $|0\rangle$ so the post-measurement state is $\rho = \frac{1}{2}\sum_{z=0}^{1} |0z\rangle\langle 0z| \otimes |0z\rangle\langle 0z| \otimes |0z\rangle\langle 0z|$.

(b) If Bob asks his box to measure in the Hadamard basis then it will measure the second qubit in the standard basis so Bob will get outcome 0 half the time and outcome 1 half the time.

If Bob asks his box to measure in the standard basis, then it will measure the first qubit in the standard basis so he will get outcome 0.

(c) Eve will get 0 since her first qubit is $|0\rangle$.

(d) Since Alice and Bob have the same state and their boxes work the same way, they must get the same outcome whenever they make the same measurement so they will pass with probability 1.

(e) Since Eve has the same state as Alice and Bob she can learn x_j by making the same measurement that Alice and Bob's boxes made: measure first qubit in standard basis if $\theta_j = 0$ and second qubit in standard basis if $\theta_j = 1$.

(f) Since Eve can recover all the x_j, $j \in T'$, Eve knows the entire key so $H_{\min}(X|E) = 0$.

Problem 3: Commuting observables are compatible.

Solution: (Due to Bolton Bailey)

(a) The two-dimensional eigenspace to which the postmeasurement state will belong will be spanned by the two Bell states which correspond to the eigenvalue -1. If we evaluate

$$(X \otimes X)|\Psi_{00}\rangle = (X \otimes X)\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|11\rangle + |00\rangle) = |\Psi_{00}\rangle$$

$$(X \otimes X)|\Psi_{01}\rangle = (X \otimes X)\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = \frac{1}{\sqrt{2}}(|11\rangle - |00\rangle) = -|\Psi_{01}\rangle$$

$$(X \otimes X)|\Psi_{10}\rangle = (X \otimes X)\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) = \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle) = |\Psi_{10}\rangle$$

$$(X \otimes X)|\Psi_{11}\rangle = (X \otimes X)\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle) = -|\Psi_{11}\rangle$$

We see that if the measurement is -1, then the post-measurement state belongs to the eigenspace spanned by $|\Psi_{00}\rangle, |\Psi_{10}\rangle$.

If we evaluate the eigenvalues for the bell states under the $Z \otimes Z$ operator

$$(Z \otimes Z)|\Psi_{00}\rangle = (Z \otimes Z)\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |\Psi_{00}\rangle$$

$$(Z \otimes Z)|\Psi_{01}\rangle = (Z \otimes Z)\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = |\Psi_{01}\rangle$$

$$(Z \otimes Z)|\Psi_{10}\rangle = (Z \otimes Z)\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) = \frac{1}{\sqrt{2}}(-|01\rangle - |10\rangle) = -|\Psi_{10}\rangle$$

$$(Z \otimes Z)|\Psi_{11}\rangle = (Z \otimes Z)\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = \frac{1}{\sqrt{2}}(-|01\rangle + |01\rangle) = -|\Psi_{11}\rangle$$

And so after the second measurement of 1, the post measurement state is $|\Psi_{01}\rangle$.

(b) If we apply $(Y \otimes Y)$ to $|\Psi_{01}\rangle$, we get $-|\Psi_{01}\rangle$, so if the post-measurement state had some overlap with this state, the measured eigenvalue would have to be -1.

(c) In general, when one measures a product of commuting observables, one gets the product of the measurement one would have gotten from each measurement indidivdually. That is,

$$\langle\psi|A|\psi\rangle\langle\psi|B|\psi\rangle = \langle\psi|AB|\psi\rangle$$

Problem 4: A coherent attack on a nonlocal game.

Solution: (Due to Anish Thilagar)

(a) They win with probability $\frac{2}{3}$. They only lose when $s = t = 0$, because then both sides of the equation evaluate to 0.

(b) There are 9 possible equally likely situations that can occur, because each game has 3 possible inputs. Both Alice and Bob follow the same strategy. If their input is $(0, 0)$, they output $(0, 0)$, and otherwise output $(1, 1)$.

Clearly, if they both output $(0, 0)$, they will fail because all 4 variable in both equations are 0. Additionally, if both of them output $(1, 1)$, they will fail because both sides of both equations will be 1.

The only remaining case is, if only one of them outputs $(0, 0)$ and the other outputs $(1, 1)$, then we have that either $a_0 \vee s_0 = a_1 \vee s_1 = 0$ and $b_0 \vee t_0 = b_1 \vee t_1 = 1$ or $a_0 \vee s_0 = a_1 \vee s_1 = 1$ and $b_0 \vee t_0 = b_1 \vee t_1 = 0$, and either way they succeed in both games, so they win. This can happen 6 different ways, because $(s_0, s_1) = (0, 0)$, then we can have $(t_0, t_1) \in \{(0, 1), (1, 0), 1, 1)\}$, and vice versa if $(t_0, t_1) = (0, 0)$. Therefore, the probability of success is $6 \times \frac{1}{9} = \frac{2}{3}$.

(c) Alice can just randomly generate values of (s_1, t_1) and send Bob t_1 and then 'forget' the value. Then, they can play the two shot game and win with probability w_c, which means they must win the one shot game with probability at least w_c, because they need to win both games to win the two shot version.

(d) First, note that A_0 and B_0 commute because they each act on separate parts of the state that are spacelike separated.

If $(s,t) = (0,0)$, which happens with probability $\frac{1}{3}$, Alice and Bob win the game with likelihood $P(a=0)P(b=1) + P(a=1)P(b=0) = P(a \neq b)$. We know that $\langle\Psi|A_0B_0|\Psi\rangle$ is the probability of the measured eigenvalues of A_0 and B_0 being the same minus the probability that they are different, because as we know from the last question the measured eigenvalue of a product of two commuting operators is the same as the product of measuring with each operator. Therefore, this tells us that $\langle\Psi|A_0B_0|\Psi\rangle = P(a=b) - P(a \neq b)$. However, $P(a=b) = 1 - P(a \neq b)$, so we have $\langle\Psi|A_0B_0|\Psi\rangle = 1 - 2P(a \neq b)$, so $P(a \neq b) = \frac{1}{2} - \frac{1}{2}\langle\Psi|A_0B_0|\Psi\rangle$ is the success probability in this case.

If $(s,t) = (0,1)$, which happens with probability $\frac{1}{3}$, they succeed exactly when $a = 0$. We know that $\langle\Psi|A_0|\Psi\rangle = P(a=0) - P(a=1)$, and using the substitution $P(a=1) = 1 - P(a=0)$, we get $P(a=0) = \frac{1}{2} + \frac{1}{2}\langle\Psi|A_0|\Psi\rangle$.

Similarly, if $(s,t) = (1,0)$, which happens with probability $\frac{1}{3}$, they succeed exactly when $b = 0$. We know that $\langle\Psi|B_0|\Psi\rangle = P(b=0) - P(b=1)$, and using the substitution $P(b=1) = 1 - P(b=0)$, we get $P(b=0) = \frac{1}{2} + \frac{1}{2}\langle\Psi|B_0|\Psi\rangle$.

Therefore, their success probability will be

$$\frac{1}{3}\left(\frac{1}{2} - \frac{1}{2}\langle\Psi|A_0B_0|\Psi\rangle + \frac{1}{2} + \frac{1}{2}\langle\Psi|A_0|\Psi\rangle + \frac{1}{2} + \frac{1}{2}\langle\Psi|B_0|\Psi\rangle\right)$$

Letting $M = \frac{1}{3}(A_0 + B_0 - A_0B_0)$, this reduces to $\frac{1}{2} + \frac{1}{2}\langle\Psi|M|\Psi\rangle$.

(e)

$$\begin{aligned} M^2 &= \frac{1}{9}(A_0 + B_0 - A_0B_0)^2 \\ &= \frac{1}{9}(A_0^2 + B_0^2 + A_0B_0 + B_0A_0 - A_0^2B_0 - B_0A_0B_0 + A_0B_0A_0B_0) \end{aligned}$$

Because A_0 and B_0 are operators, they square to identity

$$= \frac{1}{9}(2\mathbb{I} + A_0B_0 + B_0A_0 - B_0 - B_0A_0B_0 + A_0B_0A_0B_0)$$

Additionally, A_0 and B_0 commute, so we can rewrite this as

$$\begin{aligned} &= \frac{1}{9}(2\mathbb{I} + A_0B_0 + A_0B_0 - B_0 - A_0B_0^2 + A_0^2B_0^2) \\ &= \frac{1}{9}(3\mathbb{I} + 2A_0B_0 - B_0 - A_0) \\ &= \frac{1}{9}(3\mathbb{I} - 6M) \\ &= \frac{1}{3}\mathbb{I} - \frac{2}{3}M \end{aligned}$$

(f) By Cayley-Hamilton, M satisfies its characteristic polynomial, and since this is the unique monic polynomial that it satisfies, this must be its characteristic polynomial. Therefore, the eigenvalues of M will satisfy this as well, so $3\lambda^2 + 2\lambda - 1 = 0$. This factors to $(3\lambda - 1)(\lambda + 1) = 0$, so $\lambda_{\max} = \frac{1}{3}$.

(g) $p_{win} \leq \frac{1}{2} + \frac{1}{2}\langle\Psi|M|\Psi\rangle \leq \frac{1}{2} + \frac{1}{2}\frac{1}{3} = \frac{2}{3}$. We also know that this win probability is achievable even without any quantum strategy from the naive strategy in part (a), so this must be the tightest possible bound.