COM-440, Introduction to Quantum Cryptography, Fall 2025

Homework # 2 Solutions

Problems:

1. **A three-player game**

   (a) First we notice that if each player always answers 0 then they succeed with probability $\frac{3}{4}$. Next we verify that this is optimal. It suffices to consider deterministic strategies, since for every random strategy there is a deterministic one whose winning probability is at least as high (fix the best choice of random bits for everyone). If $f_A : \{0,1\} \to \{0,1\}$ is Alice's strategy (i.e. Alice answers $f_A(x)$ to x) and similarly f_B, f_C for Bob and Charlie then the chance that they answer correctly the question $(0,0,0)$ is $\frac{1}{2}+\frac{1}{2}(-1)^{f_A(0)}(-1)^{f_B(0)}(-1)^{f_C(0)}$, as can be verified by direct calculation. A similar expression is obtained for the other questions. Letting $a_x = (-1)^{f_A(x)}$ and similarly b_y, c_z we deduce that the winning probability is

   $$\frac{1}{2} + \frac{1}{8}\big(a_0b_0c_0 - a_0b_1c_1 - a_1b_0c_1 - a_1b_1c_0\big)\ .$$

   Since the product of the four quantities $a_0b_0c_0$, etc., is 1 (each variable appears exactly twice), exactly 0, 2 or 4 of them must equal -1. In all cases the entire expression is at most $\frac{3}{4}$, as claimed.

   (b) One needed to verify that

   $$\langle\psi| Z{\otimes}Z{\otimes}Z |\psi\rangle = \langle\psi| Z{\otimes}X{\otimes}X |\psi\rangle = \langle\psi| X{\otimes}Z{\otimes}X |\psi\rangle = \langle\psi| X{\otimes}X{\otimes}Z |\psi\rangle = 1\ .$$

   Everyone did this calculation correctly.

   (c) To study entanglement between Alice and Bob, we first compute the reduced density matrix between them. We obtain

   $$\rho_{AB} = \frac{1}{4}\begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ -1 & 0 & 0 & 1 \end{pmatrix}\ .$$

   At this point there are different ways to proceed. The shortest solution is to compute the rank of ρ_{AB} and verify that it is 2, not 1. Therefore the state is not pure, and cannot be maximally entangled. One could go further by showing that ρ_{AB} is in fact separable. This can be shown by using the PPT criterion, as the partial transpose of ρ_{AB} is positive and this criterion is complete in the 2×2 qubit case. (Since we hadn't reviewed this criterion in class, I didn't expect you to use it.) Another option was to find an explicit separable decomposition by observing that $\rho_{AB} = \frac{1}{2}(\mathbb{I} \otimes \mathbb{I} + Y \otimes Y)$. From there, one obtains

$$\rho_{AB} = \frac{1}{2}\big(|{+i}\rangle\langle{+i}| \otimes |{+i}\rangle\langle{+i}| + |{-i}\rangle\langle{-i}| \otimes |{-i}\rangle\langle{-i}| \big) \ ,$$

with $|{+i}\rangle$, $|{-i}\rangle$ the eigenstates of the Pauli Y matrix.

A different solution was to observe that, with respect to the bipartition AB:C, the state is locally unitarily equivalent to an EPR pair, i.e. there is maximal entanglement between (AB) and C. Because A and B are a qubit each, there could not be maximal entanglement between A and B; as then the entanglement with C would have to be zero.

Finally, since the state $|\psi\rangle$ is invariant under permutation of any two registers, the previous reasoning applies to any pair of players.

2. **Robustness of GHZ and W States**

   (a) First note that if $\rho = |\psi\rangle\langle\psi|$ is pure, then

$$\mathrm{Tr}\,(\rho\sigma) = \mathrm{Tr}\,(|\psi\rangle\langle\psi|\,\sigma) = \mathrm{Tr}\,(\langle\psi|\,\sigma\,|\psi\rangle) = \langle\psi|\,\sigma\,|\psi\rangle$$

We can view tracing out part of a state as a consequence of an unknown party, say Bob, measuring that part of the state. In this case, measuring the third qubit in the computational basis (remember that the partial trace is independent of the basis we choose) gives Bob either 0 or 1 with probability a half. The corresponding states on the first two qubits are $|00\rangle\langle 00|$ and $|11\rangle\langle 11|$, respectively. Thus, the remaining state is $\frac{1}{2}\,|00\rangle\langle 00| + \frac{1}{2}\,|11\rangle\langle 11|$. We have that $|GHZ_2\rangle\langle GHZ_2| = \frac{1}{2}\,(|00\rangle\langle 00| + |11\rangle\langle 11| + |00\rangle\langle 11| + |11\rangle\langle 00|)$, which is a pure state. Using the fact that this is a pure state, we find that

$$\begin{aligned}\mathrm{Tr}\big(\, |GHZ_2\rangle\langle GHZ_2|\mathrm{Tr}_3\, |GHZ_3\rangle\langle GHZ_3|\,\big)& \\ &= \langle GHZ_2|\,\mathrm{Tr}_3\,(|GHZ_3\rangle\langle GHZ_3|)\,|GHZ_2\rangle \\ &= \frac{1}{4}\,(\langle 00|00\rangle + \langle 11|11\rangle) = \frac{1}{2}\end{aligned}$$

   (b) Measuring the third qubit gives a 0 with probability 2/3, so that the state on the other two qubits is equal to $|W_2\rangle\langle W_2|$. If a measurement on the third qubit gives a 1 (with probability 1/3), the corresponding state on the first two qubits is $|00\rangle\langle 00|$. The state on the first two qubits after tracing out the third qubit is $\mathrm{Tr}_3\,(|W_3\rangle\langle W_3|) = \frac{2}{3}\,|W_2\rangle\langle W_2| + \frac{1}{3}\,|00\rangle\langle 00|$. Since $\langle W_2|00\rangle = 0$, we have that

$$\mathrm{Tr}\,(|W_2\rangle\langle W_2|\,\mathrm{Tr}_3\,(|W_3\rangle\langle W_3|)) = \frac{2}{3}$$

(c) We have that

$$\mathrm{Tr}_N\left(|GHZ_N\rangle\langle GHZ_N|\right) = \frac{1}{2}|\underbrace{00\ldots0}_{N-1}\rangle\langle\underbrace{00\ldots0}_{N-1}| + \frac{1}{2}|\underbrace{11\ldots1}_{N-1}\rangle\langle\underbrace{11\ldots1}_{N-1}|$$

Using similar reasoning as in the first problem, we find that the overlap is equal to 1/2. Taking the limit we also get 1/2.

(d) Measuring the last qubit gives a 0 with probability $\frac{N-1}{N}$, so that the state on the remaining qubits is equal to $|W_{N-1}\rangle\langle W_{N-1}|$. If a measurement on the last qubit gives a 1 (with probability $\frac{1}{N}$), the corresponding state on the remaining qubits is $|\underbrace{00\ldots0}_{N-1}\rangle\langle\underbrace{00\ldots0}_{N-1}|$. The state on the first $N-1$ qubits after tracing out the last qubit is then $\mathrm{Tr}_N\left(|W_N\rangle\,\langle W_N|\right) = \frac{N-1}{N}\,|W_{N-1}\rangle\langle W_{N-1}| + \frac{1}{N}|\underbrace{00\ldots0}_{N-1}\rangle\langle\underbrace{00\ldots0}_{N-1}|$. Since $\langle W_{N-1}|\underbrace{00\ldots}_{N-1}\rangle = 0$, we have that $\mathrm{Tr}\Big(\,|W_{N-1}\rangle\,\langle W_{N-1}|\,\mathrm{Tr}_N\left(|W_N\rangle\,\langle W_N|\right)\Big) = \frac{N-1}{N}$. Taking the limit we get $\lim_{N\to\infty}\frac{N-1}{N} = 1$.

3. **Nonlocal boxes**

(a) Using the equality that $\sum_a A_x^{(i),a} = \mathbb{I}$, we can get that for every set of indices $S \subseteq \{1, 2, \cdots, n\}$,

$$\begin{aligned}\sum_{a_i:i\in S} p(a_1,\cdots,a_n|x_1,\cdots,x_n) &= \sum_{a_i:i\in S}\mathrm{Tr}\big((A_{x_1}^{(1),a_1}\otimes\cdots\otimes A_{x_n}^{(n),a_n})\rho_{A_1\cdots A_n}\big)\\ &= \mathrm{Tr}\big((\sum_{a_i:i\in S} A_{x_1}^{(1),a_1}\otimes\cdots\otimes A_{x_n}^{(n),a_n})\rho_{A_1\cdots A_n}\big)\\ &= \mathrm{Tr}\big(\bigotimes_{i\in S} A_{x_i}^{(i),a_i}\rho_{A_1\cdots A_n}\big)\ ,\end{aligned}$$

which does not depend on x_i for $i \notin S$. Therefore, the non-local box is non-signaling.

A common mistake is only checking marginals on one location.

(b) Everyone did this verification correctly.

(c) (U), (PR) and (CH) are non-signaling. (SIG) is signaling.

(d) By the winning condition of CHSH game,

$$\mathbf{Pr}\left[\mathrm{Win}\right] = \frac{1}{4}\sum_{a,b,x,y\ \text{s.t.}\ a\oplus b=x\cdot y} p(a,b|x,y)\ .$$

Therefore, the success probabilities of (U), (PR), (CH) and (SIG) in the CHSH game are $\frac{1}{2}$, 1, $\cos^2\pi/8 \approx 0.85$, and 1/4, respectively.

(e) (U) can be implemented using $A_x^a = B_y^b = \mathbb{I}/2$ for every x, y, a, b, and a state $\rho_{AB} = |00\rangle\langle 00|$.

(PR) wins the CHSH game with certainty, but the optimum success probability in the CHSH game for a quantum strategy is $\cos^2 \pi/8 < 1$. Thus (PR) cannot be implemented using quantum mechanics.

(CH) can be implemented using the optimal quantum strategy for the CHSH game.

(SIG) is signaling, but by part (a), any quantum non-local box is non-signaling. So (SIG) cannot be implemented using quantum mechanics.

(f) By the non-signaling property, $\sum_{a,b} q(a,b,c|x,y,z)$ does not depend on x, y. So we can set $p'(c|z) = \sum_{a,b} q(a,b,c|x,y,z)$. We set $q(a,b|x,y) = p(a,b|x,y)$. Now let's show that $q(a,b,c|x,y,z) = p(a,b|x,y)p'(c|z)$.

Step 1: when $a \oplus b \neq x \cdot y$, $\sum_c q(a,b,c|x,y,z) = p(a,b|x,y) = 0$. As each $q(a,b,c|x,y,z) \geq 0$, we can get that when $a \oplus b \neq x \cdot y$, $\forall c, z$, $q(a,b,c|x,y,z) = 0$.

Step 2: by the non-signaling property, $\sum_b q(a,b,c|x,y,z) = \sum_b q(a,b,c|x,1-y,z)$ and $\sum_a q(a,b,c|x,y,z) = \sum_a q(a,b,c|1-x,y,z)$.

As $q(a,b,c|x,y,z) = 0$ whenever $a \oplus b \neq x \cdot y$, the above two equations can be simplified into $q(a, a \oplus (x \cdot y), c|x,y,z) = q(a, a \oplus (x \cdot (1-y)), c|x, 1-y, z)$ and $q(b \oplus (x \cdot y), b, c|x,y,z) = q(b \oplus ((1-x) \cdot y), b, c|1-x, y, z)$.

Enumerate each a, b, x, y and we can get that $q(a,b,c|x,y,z) = q(a',b',c|x',y',z)$ for every a,b,c,x,y,z,a',b',x',y' satisfying $a \oplus b = x \cdot y$ and $a' \oplus b' = x' \cdot y'$.

Step 3: now let's verify that $q(a,b,c|x,y,z) = p(a,b|x,y)p'(c|z)$. For $a \oplus b \neq x \cdot y$, both sides are 0 and thus are equal. For $a \oplus b = x \cdot y$, $q(a,b,c|x,y,z) = \frac{1}{2}(q(a,b,c|x,y,z) + q(1-a,1-b,c|x,y,z))$ (by step 2), which is exactly $p(a,b|x,y)p'(c|z)$.

Hence any non-signaling tripartite extension of (PR) must have a product form.

(g) The optimum success probability achieved by any non-signaling tripartite box in the CHSH game is 3/4.

On one hand, the non-signaling tripartite box that always outputs 0 ($p(0,0,0|x,y,z) = 1$ for every x, y, z) wins the game with probability 3/4.

On the other hand, similar as (d), we can write the success probability as

$$\mathbf{Pr}\,[\text{Win}] = \frac{1}{24}\left(\sum_{a,b,c,x,y,z \text{ s.t. } a\oplus b = x\cdot y} p(a,b,c|x,y,z) + \sum_{a,b,c,x,y,z \text{ s.t. } b\oplus c = y\cdot z} p(a,b,c|x,y,z) \right.$$
$$\left. + \sum_{a,b,c,x,y,z \text{ s.t. } c\oplus a = z\cdot x} p(a,b,c|x,y,z)\right),$$

which is linear in each $p(a,b,c|x,y,z)$.

Besides, all the constraints for a family of distributions to be a non-local box are linear in $p(a,b,c|x,y,z)$.

Therefore, we can use the linear programming to solve the problem, and the result is 3/4.