CS120, Quantum Cryptography, Fall 2016

Homework # 2 **due: 10:29AM, October 18th, 2016**

Ground rules:

Your homework should be submitted to the marked bins that will be by Annenberg 241.

Please format your solutions so that each problem begins on a new page, and so that your name appears at the top of each page.

You are strongly encouraged to collaborate with your classmates on homework problems, but each person must write up the final solutions individually. You should note on your homework specifically which problems were a collaborative effort and with whom. You may not search online for solutions, but if you do use research papers or other sources in your solutions, you must cite them.

Late homework will not be accepted or graded. Extensions will not be granted, except on the recommendation of a dean. We will grade as many problems as possible, but sometimes one or two problems will not be graded. Your lowest homework grade of the quarter will be dropped from your final grade.

Place all your problems in the first (top) bin in the box by Annenberg 241. Start each problem on a new page, with your name clearly marked at the top of the page.

Problems:

1. (3 points) **Classical one-time pad**

   We meet up again with our favourite protagonists, Alice and Bob. As you've seen in class, Alice and Bob have an adversary named Eve who is intent on listening in on all the conversations Alice and Bob have. In order to protect themselves, they exchange a classical key $k = k_1 k_2 \dots k_n$ which they can use to encrypt messages and hence be safe from Eve. Alice knows that a safe way to encode messages would be to use a classical one time pad, as seen in the lecture notes. But she feels like this uses a large amount of key, and being a smart student she comes up with the following encoding scheme which she claims is also secure but uses less key. Alice's scheme goes as follows.

   Alice's message is an n-bit string $m = m_1 m_2 \dots m_n$. For i from 1 to n,

   1) Alice flips a fair coin.
   2) If the result is tails, she sets $c_i = m_i \oplus k_i$.
   3) If the result is heads, she sets $c_i = m_i \oplus r$, where r is a fresh random bit.

   The encrypted ciphertext is $c = c_1 c_2 \dots c_n$.

(a) How many bits of key will Alice use on average with the new protocol?

(b) Is this protocol correct? Is it secure? Provide a proof of security or an attack scheme.

2. (3 points) **Superpositions and mixtures**

Alice wants to send the state $|0\rangle$ to Bob. But 50% of the time, her (noisy) device outputs the state $|1\rangle$ instead.

(a) Give the density matrix ρ_0 describing Bob's state.

(b) Suppose Bob measures ρ_0 in the standard basis. What is the probability that the measurement results in $|0\rangle$? $|1\rangle$? What if Bob measures in the Hadamard basis?

(c) Now say that the machine on Alice's side is not noisy but simply misaligned: it consistently prepares qubits in the state $|+\rangle$. Again, what is the distribution of outcomes if Bob measures in the standard basis? In the Hadamard basis?

3. (2 points) **Quantum one-time pad**

In the lecture notes, you saw that two classical bits of key suffice to encrypt one quantum bit. On an intuitive level, our scheme needed to use both the X and Z gates because the X operation has no effect on the $|+\rangle$ state and the Z operation has no effect on the $|0\rangle$ state. Alice decides to avoid this problem by using H, which fixes neither $|0\rangle$ nor $|+\rangle$. Explicitly, she uses the following protocol to encode a qubit $|\psi\rangle$: Let $k \in \{0, 1\}$ be the key bit. Encrypt $|\psi\rangle$ as $H^k |\psi\rangle$.

(a) Is this protocol a correct encryption scheme?

(b) Is this protocol a secure encryption scheme? Provide either a proof of security or an attack.

4. (6 points) **Unambiguous quantum state discrimination**

(adapted from Nielsen and Chuang)

In this problem we explore an essential practical advantage that comes with general POVMs rather than strictly projective measurements. Consider the following scenario: Bob sends Alice a qubit prepared in one of the two non-orthogonal states $|0\rangle$ and $|+\rangle$. Alice wants to perform a measurement on this qubit that distinguishes it as either $|0\rangle$ or $|+\rangle$ as *soundly* as possible, i.e. with minimum probability of mis-identifying $|0\rangle$ as $|+\rangle$ or vice versa. Let us first restrict her to projective measurements.

(a) Suppose Alice measures in the basis $\{|0\rangle, |1\rangle\}$. She identifies the state as $|0\rangle$ if she gets the outcome $|0\rangle$ and as $|+\rangle$ if she gets the outcome $|1\rangle$. What is her probability of misidentifying the state given that it is $|0\rangle$? What is her probability of misidentifying the state given that it is $|+\rangle$?

(b) Suppose instead Alice measures in the basis $\{|+\rangle, |-\rangle\}$. She identifies the state as $|+\rangle$ if she gets the outcome $|+\rangle$ and as $|0\rangle$ if she gets the outcome $|-\rangle$. Again, what are her probabilities of misidentifying the state in each case?

(c) Is it possible for Alice to do better than this with any projective measurement? Assume $|0\rangle$ and $|+\rangle$ are equally likely a priori.

Now suppose we allow Alice to perform a general measurement. In particular consider the following POVM with three elements:

$$E_1 = \frac{\sqrt{2}}{1+\sqrt{2}} |1\rangle\langle 1|$$
$$E_2 = \frac{\sqrt{2}}{1+\sqrt{2}} \frac{(|0\rangle - |1\rangle)(\langle 0| - \langle 1|)}{2}$$
$$E_3 = \mathbb{I} - E_1 - E_2$$

Alice identifies the state as $|+\rangle$ if she gets outcome 1, as $|0\rangle$ if she gets outcome 2, and makes no identification if she gets outcome 3.

(d) What is her probability of mis-identifying the state? What is her probability of failing to make an identification?

(e) Is there any POVM that gives Alice a better chance of making a correct identification *without* increasing the chance of making an incorrect identification?

5. (4 points) **Robustness of GHZ and W States**

In this problem we explore two classes of N-qubit states that are especially useful for cryptography and communication, but behave very differently under tracing out a single qubit. Let's first define them for $N = 3$:

$$\text{GHZ state:} \quad |GHZ_3\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$$
$$\text{W state:} \quad |W_3\rangle = \frac{1}{\sqrt{3}}(|100\rangle + |010\rangle + |001\rangle)$$

Note that both states are invariant under permutation of the three qubits, so without loss of generality we may trace out the last one. We'll denote this operation by Tr_3. Also, we have analogous definitions in the two-qubit case: $|GHZ_2\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and $|W_2\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle)$.

In the following we consider the *overlap* between N-qubit GHZ and W states with one qubit discarded (i.e. traced out) and their $(N-1)$-qubit counterparts. The overlap of density matrices ρ and σ is defined as $\mathrm{Tr}\,\rho\sigma$, a measure of "closeness" that generalizes the expression $|\langle\phi|\psi\rangle|^2$ for pure states.

(a) Calculate the overlaps

(i) $\mathrm{Tr}(|GHZ_2\rangle\langle GHZ_2| \,\mathrm{Tr}_3\, |GHZ_3\rangle\langle GHZ_3|)$ and

(ii) $\mathrm{Tr}(|W_2\rangle\langle W_2| \,\mathrm{Tr}_3\, |W_3\rangle\langle W_3|)$.

Now we generalize to the N-qubit case. As you might expect, $|GHZ_N\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes N} + |1\rangle^{\otimes N})$ and $|W_N\rangle$ is an equal superposition of all N-bit strings with exactly one 1 and $N-1$ 0's.

(b) Calculate the following overlaps as functions of N.

(i) $\mathrm{Tr}(|GHZ_{N-1}\rangle\langle GHZ_{N-1}| \,\mathrm{Tr}_N\, |GHZ_N\rangle\langle GHZ_N|)$ and

(ii) $\mathrm{Tr}(|W_{N-1}\rangle\langle W_{N-1}| \,\mathrm{Tr}_N\, |W_N\rangle\langle W_N|)$

Conclude that W states are "more robust" against loss of a single qubit than GHZ states.

6. (6 points) **Universal Cloning**

In this problem we analyze a single-qubit *universal cloner*.

(a) Consider the map which takes as input a pure single-qubit state $\rho = |\psi\rangle\langle\psi|$, and returns $T_1(\rho) = \rho \otimes \frac{1}{2}\mathbb{I}$, where $\frac{1}{2}\mathbb{I}$ is the maximally mixed state of a single qubit.

(i) Show that this map is a valid quantum operation: it is CPTP. Give an interpretation of this map in terms of making a random guess for the cloned qubit.

(ii) Evaluate the success probability $|\langle\psi|\langle\psi| T_1(|\psi\rangle\langle\psi|)|\psi\rangle|\psi\rangle|$ of this cloner (for any state $|\psi\rangle$ — your answer should not depend on $|\psi\rangle$).

(b) Let's consider a second cloning map, which acts on the qubit input state together with two ancilla qubits as follows:

$$U : |0\rangle|0\rangle|0\rangle \mapsto \sqrt{\frac{2}{3}}|0\rangle|0\rangle|0\rangle + \sqrt{\frac{1}{6}}\big(|0\rangle|1\rangle + |1\rangle|0\rangle\big)|1\rangle\,,$$
$$|1\rangle|0\rangle|0\rangle \mapsto \sqrt{\frac{2}{3}}|1\rangle|1\rangle|1\rangle + \sqrt{\frac{1}{6}}\big(|1\rangle|0\rangle + |0\rangle|1\rangle\big)|0\rangle\,.$$

(i) Verify that U can be extended into a valid three-qubit unitary.

The cloning map associated to U is the map T_2 which first initializes two qubits to the $|0\rangle|0\rangle$ state, then applies U, and then traces out the third qubit.

(ii) Evaluate the success probability of the map U on an arbitrary input pure state $\rho = |\psi\rangle\langle\psi|$.

(c) Consider a third cloning map T_3 defined as $T_3(\rho) = \frac{2}{3}P_+(\rho\otimes\mathbb{I})P_+$, where $P_+ = \mathbb{I} - |\Psi_-\rangle\langle\Psi_-|$ and $|\Psi_-\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle - |1\rangle|0\rangle)$.

(i) Verify that T_3 is a CPTP map.

(ii) Evaluate its success probability as a universal cloning map.

(iii) Is this a coincidence — is there a relationship between the three maps you have considered?