Physics 572: Homework #2

Due Date: April 4$^{\text{th}}$, 2019

Problem 1: Quantum Money. In this problem we will analyze attacks on Weisner's quantum money scheme which are based on *approximately* cloning the unknown quantum money state. Consider a quantum bank note that is a single qubit in one of the states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, chosen uniformly at random. The counterfeiter will act on the bank note with some quantum channel in order to output two qubits which will (separately) be submitted to the bank for verification. The attack succeeds if and only if *both* of the counterfeit notes are accepted by the bank. If the probability for both qubits to pass the verification test is p, then the counterfeiter can repeat the attack n times to pass the test for an n-qubit Weisner bank note with probability p^n.

(I. (10 points) The counterfeiter applies an attack based on measurement. The note is measured in the $\{|0\rangle, |1\rangle\}$ basis, and two copies of the measured state are submitted to the bank for verification (e.g. if the measurement yields "1", then the counterfeiter submits the state $|11\rangle$). What is the probability (averaged over all possible input bank notes) for the counterfeiter to succeed?

(II. (20 points) This time the counterfeiter takes the quantum bank note $|\$\rangle$, appends a qubit in the state $|0\rangle$, applies a CNOT and submits the resulting state,

$$\left(|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X\right) |\$\rangle|0\rangle \tag{1}$$

to the bank for verification. What is the success probability for this attack?

(III. (20 points) The counterfeiter takes the bank note $|\$\rangle$, prepends two qubits in the $|0\rangle$ state to obtain $|00\$\rangle$, and the applies the three qubit unitary map which acts as

$$|000\rangle \mapsto \frac{\sqrt{3}}{2}|000\rangle + \frac{|110\rangle + |101\rangle + |011\rangle}{\sqrt{12}}, \tag{2}$$

$$|001\rangle \mapsto \frac{\sqrt{3}}{2}|111\rangle + \frac{|001\rangle + |010\rangle + |100\rangle}{\sqrt{12}}, \tag{3}$$

and acts as the identity on all other computational basis states (e.g. $|100\rangle \mapsto |100\rangle$). After applying this unitary, the counterfeiter submits the first two qubits to the bank for verification. What is the success probability for this attack?

Note: The attack described above achieves the optimal probability of successfully counterfeiting notes in Weisner's quantum money scheme.

Problem 2: Quantum Key Distribution. In the BB84 QKD protocol Alice generates two random n-bit strings a and b, and then uses b to determine the basis she will use to encode the string a before sending it. Bob now samples a random n-bit string b', which determines the measurement bases that he will choose, and he obtains the n-bit string of measurement results a'. After Bob has received all the qubits and completed his measurements, Alice announces b, and Bob announces the string $b \oplus b'$ i.e. the locations in which b and b' differ. Finally, they discard the entries of a and a' where b and b' differ.

A practical challenges to the BB84 QKD scheme is the difficulty of reliably generating and detecting single photons. If Alice thinks she is sending a single photon, but accidentally sends multiple identical photons, then an eavesdropper Eve could conceivably siphon off these extra photons and store them until b is announced. Then Eve could look use b to measure her stored photons in the right bases. In this problem we will analyze a variant of BB84 in which Alice avoids ever publicly announcing her string b. This will increase the number of photons that Eve would need to steal in the above scenario in order to learn the secret key.

I. (10 points) Alice generates $a = 011001$ and $b = 101011$. She sends a 6 qubit state $|\psi\rangle$ to Bob as follows: for the i-th qubit, if $b_i = 0$ she sends $|a_i\rangle$, and if $b_i = 1$ she sends $H|a_i\rangle$ where H is the Hadamard gate. Alice sends these qubits to Bob, who then samples the bit string $b' = 100111$ and measures each qubit of $|\psi\rangle$ in the basis specified by the corresponding entry of b'. Finally, Alice announces b and Bob announces where $b \oplus b'$. What secret key are they left with?

II. (10 points) If Alice and Bob perform the same protocol with n-bit strings a, a', b, b' which are chosen uniformly at random, then what is the expected length of the secret key they obtain?

III. (10 points) In a variant of BB84 called SARG04, Alice avoids announcing her string b. Instead, for each qubit in $|\psi\rangle$ she sends a classical description of a random pair

$$\{0, |+\rangle\} \quad , \quad \{|0\rangle, |-\rangle\} \quad , \quad \{|1\rangle, |+\rangle\} \quad , \quad \{|1\rangle, |-\rangle\} \tag{4}$$

such that her qubit is in the pair. Bob then analyzes this string of pairs, and determines the locations in which his measurement result unambiguously determines which of the qubit states Alice sent. He announces these positions and then Alice and Bob use the corresponding entries of a, a' as their secret key. Give an example of a string of pairs that Alice could send, and the resulting key that Alice and Bob construct.

IV. (10 points) If Alice and Bob perform the SARG04 protocol described above with n-bit strings a, a', b, b' which are chosen uniformly at random, then what is the expected length of the secret key they obtain from this protocol?

V. (10 points) Alice is runnning QKD on a noisy experimental apparatus that sends a single photon 99% of the time, but the other 1% of the time she accidentally sends two copies of the same photon. Any time an extra photon is sent, Eve will collect and store it. After Alice and Bob make their announcements according to the SARG04 protocol, Eve measures her photons to learn as much about the secret key as possible. What is the expected number of bits of the secret key that Eve can guess correctly?

Problem 3: Noisy Teleportation.

I. (20 points) To teleport a single qubit state to Bob, Alice performs a Bell measurement and then sends two bits of classical information c_1c_2 to Bob which allow him to descramble the quantum state she intended to send. Let them agree on the table:

State	c_1	c_2
$\vert\Phi^+\rangle = \frac{1}{\sqrt{2}} = (\vert 00\rangle + \vert 11\rangle)$	0	0
$\vert\Phi^-\rangle = \frac{1}{\sqrt{2}} = (\vert 00\rangle - \vert 11\rangle)$	0	1
$\vert\Psi^+\rangle = \frac{1}{\sqrt{2}} = (\vert 01\rangle + \vert 10\rangle)$	1	0
$\vert\Psi^-\rangle = \frac{1}{\sqrt{2}} = (\vert 01\rangle - \vert 10\rangle)$	1	1

Alice and Bob share a noisy classical channel that sometimes loses bits. Consider a scenario in which Bob only receives c_1 (and he knows it came through uncorrupted) but he does not receive c_2 (e.g. there was no signal received at the agreed upon time for sending c_2). What Pauli correction does Bob apply based on his knowledge of c_1, and what is the resulting quantum state?

II. (15 points) In this scenario Alice and Bob have access to qutrits, with computational basis states labeled $|\tau\rangle$ with $\tau \in \{0, 1, 2\}$. They only have access to a limited set of operations. They can perform arbitrary single qutrit rotations, for example to prepare the state

$$|+\rangle_\tau = \frac{1}{\sqrt{3}} (|0\rangle + |1\rangle + |2\rangle) \tag{5}$$

But the only operation they can perform jointly on two qutrits is a projection onto the subspace $\text{span}\,(|\tau_1\tau_2\rangle : \tau_1 + \tau_2 = 0 \bmod 3)$,

$$\Pi_{\tau_1+\tau_2=0} = |00\rangle\langle 00| + |12\rangle\langle 12| + |21\rangle\langle 21|. \tag{6}$$

They implement this projection by trial and error using a quantum channel and a measurement, and then discarding and starting over if it does not project onto the subspace described above. Show that Alice and Bob can prepare states of the form

$$|\Phi\rangle = \frac{1}{\sqrt{3}} (|00\rangle + |12\rangle + |21\rangle), \tag{7}$$

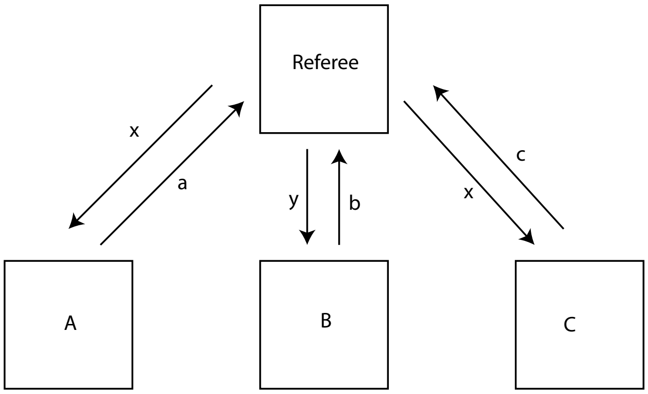
and comment on whether Alice and Bob are capable of generating entanglement with the limited operations available to them.

III. (15 points) Suppose Alice holds an arbitrary qutrit state,

$$|\psi\rangle = c_0|0\rangle + c_1|1\rangle + c_2|2\rangle \tag{8}$$

and also shares a state $|\Phi_{AB}\rangle$ of the form (7) with Bob. Design a protocol using the available operations to show that Alice can, with some probability of success, "incoherently teleport" her state to Bob so that he receives the state

$$\rho = |c_0|^2|0\rangle\langle 0| + |c_1|^2|1\rangle\langle 1| + |c_2|^2|2\rangle\langle 2|. \tag{9}$$



Problem 4: Nonlocal Games and Entangled Strategies. Consider a nonlocal game involving three players A, B, C who interact with a referee. The referee will send a single bit to each of the respective players (A gets question bit x, B gets y, C gets z), with the promise that

$$x + y + z = 0 \pmod 2 \tag{10}$$

The goal for the players, who cannot communicate with one another because this is a nonlocal game, is to return respective bits a, b, c (see the figure above) which satisfy

$$(a + b + c) = \mathrm{OR}(x, y, z) \pmod 2, \tag{11}$$

i.e. the parity of a, b, c should be odd if and only if at least one of the bits x, y, z is equal to 1.

I. (15 points) What is the optimal success probability for a classical deterministic strategy?

II. (15 points) Suppose the three players initially hold the quantum state,

$$|\psi\rangle = \frac{1}{2}\left(|000\rangle - |011\rangle - |101\rangle - |110\rangle\right)_{ABC}, \tag{12}$$

and apply the following strategy. If a player receives the question bit 0 they measure their qubit in the $\{|0\rangle, |1\rangle\}$ and return the outcome as their response. Otherwise, if a player receives the question bit 1 they apply a Hadamard rotation to their qubit and then measure in the $\{|0\rangle, |1\rangle\}$ basis and return that outcome. Show that this strategy lets them win the game with probability 1.

III. (20 points) Instead of (12), suppose the players share the Greenberger–Horne–Zeilinger (GHZ) state,

$$|\psi_{\mathrm{GHZ}}\rangle = \frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right) \tag{13}$$

Devise a strategy which allows the players to win with probability 1. **Hint:** all three players will perform a single qubit measurement $\{M_0, I - M_0\}$ if they receive the question bit 0, and $\{M_1, I - M_1\}$ if they received the question bit 1. Your goal is to find M_0 and M_1.

Remark: The existence of perfect quantum strategies that win the game with probability 1, while no classical strategies can be perfect, is both theoretically remarkable and experimentally advantageous.