Quantum Computing 2019 Set 3

Due November ~~21st~~ 25th

Instructions: Solutions should be legibly handwritten or typset. Sets are to be returned in the mailbox outside 615 Soda Hall.

If you need more time on this set, make sure to email Chinmay your set instead of handing it in on paper as he is travelling Nov 26th - Dec 7th.

Problem 1 (Quantum money)**.** Consider a bank trying to produce an information theoretically secure bill. They decide to use quantum information to their advantage. Each bill is a pair $\$ = (|\phi_s\rangle, s)$ where $|\phi_s\rangle \in (\mathbb{C}^2)^{\otimes n}$ is a quantum state and s is a classical serial number for the bill.

The states $|\phi_s\rangle$ is not too complex; it is

$$|\phi_s\rangle = H^{a_s} X^{b_s} |0\rangle^{\otimes n}$$

where $a_s, b_s \in \{0,1\}^n$ are classical strings held by the bank and chosen uniformly randomly[1].

The bank offers the following service: it allows a client to come to the bank and verify the legitimacy of a bill. To verify a bill, the bank measures all n qubits — the ith qubit in the Z-basis if $a_s(i) = 0$ and the X-basis if $a_s(i) = 1$ and ensures the measurement is $b_s(i)$. If all the measurements pass, the bank returns the bill to the client. If the measurements fail, the bank calls the police to arrest the client ($-\infty$ value to the client) .

1. **(1 point)** Show that from the client's perspective, the quantum states of two bills $|\phi_s\rangle$ and $|\phi_{s'}\rangle$ are indistinguishable.

2. **(2 points)** Assume we have access to one bill $\$_0 = (|\phi_s\rangle, s)$. Show that we cannot from this bill make two quantum states $|\psi_1\rangle, |\psi_2\rangle$ such that the two bills $\$_1 = (|\psi_1\rangle, s)$ and $\$_2 = (|\psi_2\rangle, s)$ are accepted by the bank. Formally, let V be the verification procedure employed by the bank. Show that

$$\Pr\left(V(\$_1) \text{ and } V(\$_2) \text{both pass}\right) = \exp(-n).$$

[1] Here, we employ the notation $H^a = H^{a(1)} \otimes H^{a(2)} \otimes \ldots \otimes H^{a(n)}$, etc.

3. **(2 points)** Show that if the bank does not call the police to arrest the client but instead returns the "failed" bill back to the client with an error message that an adversary can duplicate a bill.

4. **(2 points)** Now assume that the cost of going to jail isn't $-\infty$ but rather some constant $-C$. Assume the value of the bill is 1. We will find an attack that duplicates a bill with only a small probability p of getting caught (the length of the attack will depend on p and n). Therefore, for choice of $p < 1/C$, this attack has positive expectation.

   Since the qubits of $|\phi_s\rangle$ are in tensor product, our attack will determine the value of each qubit one-by-one. We first come up with a test to determine if the ith qubit $|\phi_s(i)\rangle$ is $|+\rangle$.

   Let $|\theta\rangle = \cos\theta\,|0\rangle + \sin\theta\,|1\rangle$ and let U_θ be the unitary rotating by angle θ:

   $$U_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}. \qquad (\star)$$

   We start with an additional control qubit $|g\rangle = |0\rangle$ and then apply the following transformation to $|g\rangle \otimes |\phi_s(i)\rangle$

   $$\mathrm{CNOT}(U_\theta \otimes \mathbb{I})$$

   and send the second qubit as our ith qubit to the bank for verification. What occurs in the four cases $|\phi_s(i)\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$?

5. **(2 points)** Let T be even and satisfy $T\theta = \pi/2$. Consider repeating the process T times of applying $(\star)$ and sending the second qubit for verification. For each of the four cases, what will be the measurement outcome of the control qubit after this process and what is the probability of getting arrested?

6. **(2 points)** Conclude with a strategy that calculates the classical description of the state $|\phi_s\rangle$ and that gets arrested with probability $< 1/C$. How many times did the bank need to run the verification procedure?

Historical context: This scheme was originally proposed by Wiesner in 1968 and was thought to be an unbreakable scheme for private-key quantum money. The attack in steps 4-6 is from a result by Brodutch, Nagaj, Sattath and Unruh in 2016 and is a variant of the Elitzur-Vaidman bomb testing paradox.

Problem 2 (Understanding Grover's)**.**

1. **(2 points)** Give a circuit for running Grover's search on 2 qubits where $f(x) = 1$ for exactly one $x \in \{0,1\}^2$. What is the probability of finding x?

2. **(4 points)** Consider an f where there M solutions to $f(x) = 1$ for $x \in \{0,1\}^n$. What happens if someone impatiently runs Grover's search by measuring the state of the quantum algorithm between each iteration of Grover's search to see if it has found a solution yet? Formally, between each Grover iteration, they measure according to the following POVM:

$$\left\{ M_0 = \sum_{x:f(x)=0} |x\rangle\langle x| \, , M_1 = \sum_{x:f(x)=1} |x\rangle\langle x| \right\}.$$

   How long does Grover's take now?

Problem 3 (Stabilizer Codes)**.** Recall that a CSS code is a code where all the stabilizers are either 'X'-type or 'Z'-type, meaning that each stabilizer is a tensor product of only identity and X gates or is a tensor product of only identity and Z gates, respectively. Similarly, we can say a "CSS state" is a stabilizer state for which stabilizer generators either are tensor products of only identity and X gates or tensor products of only identity and Z gates.

Let $|\psi\rangle$ be a CSS state and take $|\psi\rangle \otimes |\psi\rangle$ and apply CNOT gates from each qubit j of the first copy to qubit j of the second copy.

1. **(2 points)** What does this transformation do?

2. **(2 points)** What does this transformation do when there is an X error on the first qubit of the first copy? Meaning the initial state is instead

$$(X_1 |\psi\rangle) \otimes |\psi\rangle \, .$$