COL872: Quantum and Post-Quantum Cryptography

Problem Set 3

Due date: March 14th, 2023

Instructions

1. Assignments must be done in groups of size at most three. Each group must upload one submission, and mention the names of all group members.
2. You are welcome to discuss with other classmates and instructor, as well as refer to resources online. But if you do, please mention who all you collaborated with, or the online resources used.

This is version 1 of the assignment, uploaded on 04/03/23.

Questions

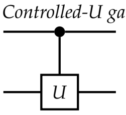
Question 1. ***Controlled Unitaries*** *(5 marks)*

In Lecture 14, we discussed how to implement a 'controlled Z' gate. One of the students asked if it is possible to implement a 'controlled U' gate for any unitary $\mathbf{U}$*. In this problem, we will study this question for single-qubit unitaries. Let* $\mathbf{U} \in \mathbb{C}^{2\times 2}$ *be a unitary operation over single qubit. For any such unitary, there exist unitary matrices* $\mathbf{A}, \mathbf{B}, \mathbf{C}$ *and* α *such that*

$$\mathbf{A}\cdot\mathbf{B}\cdot\mathbf{C} = \mathbf{I} \text{ and } \mathbf{U} = e^{i\alpha}\mathbf{A}\cdot\mathbf{X}\cdot\mathbf{B}\cdot\mathbf{X}\cdot\mathbf{C}$$

Let $\mathbf{U} = \mathbf{A}\cdot\mathbf{X}\cdot\mathbf{B}\cdot\mathbf{X}\cdot\mathbf{C}$ *where* $\mathbf{A}\cdot\mathbf{B}\cdot\mathbf{C} = \mathbf{I}$*. Use this representation to construct a 'controlled U' gate using* CNOT*, and gates implementing the unitaries* $\mathbf{A}, \mathbf{B}, \mathbf{C}$*. Compute all intermediate steps of the computation, and prove that it indeed implements the 'controlled U' gate.*

Controlled-U gate:



See Corollary 4.2 in [NC16] for a proof of this fact.

Question 2. ***Standard Oracle vs Controlled Phase Oracle*** *(5 marks)*

Let $f : \{0,1\}^n \to \{0,1\}$ *be a classical function, and let* $\mathbf{U}_f$ *be the unitary such that* $\forall x \in \{0,1\}^n, y \in \{0,1\}, \mathbf{U}_f |x\rangle |y\rangle = |x\rangle |y \oplus f(x)\rangle$.

In class, we saw that the phase oracle can be implemented using $\mathbf{U}_f$*. Consider the* controlled phase *unitary* CP_f *that behaves as follows:*

$$\forall x \in \{0,1\}^n, y \in \{0,1\}, \mathsf{CP}_f \left|x\right\rangle \left|y\right\rangle = (-1)^{y \cdot f(x)} \left|x\right\rangle \left|y\right\rangle$$

1. *Show that, for any* $f : \{0,1\}^n \to \{0,1\}$*,* $\mathbf{U}_f$ *can be implemented using* CP_f*.*
2. *Show that, for any* $f : \{0,1\}^n \to \{0,1\}$*,* CP_f *can be implemented using* U_f*.*

Question 3. ***Measurements, and Principle of Deferred Measurements*** *(5 points)*

1. *Construct a single qubit quantum circuit such that it has identical output on* $\left|0\right\rangle$ *and* $\left|1\right\rangle$*, but different output on* $\left|+\right\rangle$*.*

In class, we saw a couple of examples to delay all measurements until the end of the computation.

2. *Show that any quantum circuit* C *oeprating on* n *qubits with* m *intermediate measurement gates can be perfectly simulated using a quantum circuit* C' *acting on* $n+m$ *qubits such that all measurements happen at the end of the computation.*

Question 4. ***Modified Simon's Problem*** *(5 marks)*
Design an efficient quantum algorithm for the 'Modified Simon's Problem'. Here, the algorithm is given oracle access to two functions $f_1 : \{0,1\}^n \to \{0,1\}^n, f_2 : \{0,1\}^n \to \{0,1\}^n$ *with the guarantee that there exists a bit-string* $\mathbf{s} \in \{0,1\}^n$ *such that for all* $\mathbf{x} \in \{0,1\}^n$*,* $f_1(\mathbf{x}) = f_2(\mathbf{x} \oplus \mathbf{s})$*. The algorithm must output* $\mathbf{s}$ *with non-negligible probability, and can make* $\mathrm{poly}(n)$ *queries to* f_1, f_2*. Describe the quantum circuit using unitaries* U_{f_1}, U_{f_2}*.*

Question 5. ***Encrypting a quantum state using classical keys*** *(7 marks)*
In one of the initial lectures, we discussed how to encrypt a single qubit using two classical bits.

- $\mathsf{Enc}(k = (a,b), \left|\psi\right\rangle)$*: Output* $\mathbf{X}^a\mathbf{Z}^b \left|\psi\right\rangle$*.*

We will prove that this encryption scheme guarantees perfect secrecy. Therefore, it is similar to the classical one-time pad. Classically, we required a single bit key to perfectly encrypt a single bit message. Here, we require two classical bits for perfectly encrypting a single qubit message.

1. *Consider an operator that maps a matrix* $\mathbf{M} \in \mathbb{C}^{2\times 2}$ *to*

$$\frac{1}{4}\left(\mathbf{M} + \mathbf{X}\cdot\mathbf{M}\cdot\mathbf{X} + \mathbf{Z}\cdot\mathbf{M}\cdot\mathbf{Z} + \mathbf{X}\cdot\mathbf{Z}\cdot\mathbf{M}\cdot\mathbf{Z}\cdot\mathbf{X}\right).$$

What is the output when this operator is applied to $\mathbf{M} \in \{\mathbf{I}, \mathbf{X}, \mathbf{Z}, \mathbf{X}\cdot\mathbf{Z}\}$*?*

2. *Show that any density matrix $\rho \in \mathbb{C}^{2\times 2}$ can be expressed as a linear combination of $\mathbf{I}, \mathbf{X}, \mathbf{Z}, \mathbf{X} \cdot \mathbf{Z}$.*

3. *Suppose we encrypt a quantum state $|\psi\rangle$ using a random 2-bit key (a, b). The resulting density matrix is*

$$\rho = \frac{1}{4}\left(|\psi\rangle\langle\psi| + \mathbf{X}\,|\psi\rangle\langle\psi|\,\mathbf{X} + \mathbf{Z}\,|\psi\rangle\langle\psi|\,\mathbf{Z} + \mathbf{X}\cdot\mathbf{Z}\,|\psi\rangle\langle\psi|\,\mathbf{Z}\cdot\mathbf{X}\right).$$

   Using the above two parts, what can we conclude about ρ?

4. *The above encryption scheme can be extended to encrypt any m qubit state using $2m$ classical bits. Propose a public key encryption scheme that can encrypt any quantum state $|\psi\rangle$ (over m qubits, where m is unbounded).*
   As in the classical setting, we will have only computational security, and the security depends on the key length. You don't need to prove security here.

Question 6. ***Schmidt Decomposition*** *(5 marks)*

Let $|\psi\rangle$ be any pure state over $2n$ qubits. The state $|\psi\rangle$ can be expressed as $\sum_{x,y\in\{0,1\}^n} \alpha_{x,y}\,|x\rangle\,|y\rangle$. These coefficients $\{\alpha_{x,y}\}$ can be any complex number. Interestingly, there exists a 'nice' decomposition, known as Schmidt decomposition, using which we can assume that these coefficients are positive. There exist two sets of orthonormal vectors $\{|u_i\rangle\}_i$ and $\{|v_i\rangle\}_i$ and positive Schmidt coefficients $\{\lambda_i\}_i$ such that

See Section 2.5 in [NC16] for a proof of this decomposition.

$$|\psi\rangle = \sum_i \lambda_i\,|u_i\rangle\,|v_i\rangle$$

Here, we will see two consequences of this decomposition.

1. *Let ρ be the density matrix for a mixed state over n qubits. In class, we saw that there exists a pure state $|\psi\rangle$ over $2n$ qubits such that measuring the last n qubits results in the density matrix ρ. Using Schmidt decomposition, prove that if $|\psi_1\rangle$ and $|\psi_2\rangle$ are two purifications of ρ, then there exists a unitary matrix $\mathbf{U}$ acting over n qubits such that $|\psi_2\rangle = (\mathbf{I}_n \otimes \mathbf{U})\,|\psi_1\rangle$. Here $\mathbf{I}_n$ is the identity operation over the first n qubits.*

2. *Let ρ_1, ρ_2 be two density matrices, corresponding to mixed states over n qubits. Show that the following two statements are equivalent:*

   - *ρ_1 and ρ_2 have the same set of eigenvalues (counting multiplicities).*
   - *There exists a pure state $|\psi\rangle$ over $2n$ qubits such that when the first n qubits are measured, the state of the remaining qubits is described by density matrix ρ_2. Similarly, when the last n qubits are measured, the state of the first n qubits is ρ_1.*

Question 7. ***General Measurements*** *(8 points)*

Projective measurements are a generalization of (partial) measurements that we saw in class. A projective measurement is defined using t Hermitian matrices $\mathcal{P} =$

Hermitian: $\mathbf{M} = \mathbf{M}^\dagger$

$\{\mathbf{P}_i\}_{i\in[t]}$. Each of these $\mathbf{P}_i$ matrices satisfies $\mathbf{P}_i^2 = \mathbf{P}_i$. Moreover, $\mathbf{P}_i \cdot \mathbf{P}_j = \mathbf{0}$ and $\sum_i \mathbf{P}_i = \mathbf{I}$.

On applying the measurement, the measurement produces a classical output (which is an integer $i \in [t]$) and a quantum state. When the measurement $\mathcal{P}$ is applied on state $|\psi\rangle$, the index i is output with probability $\langle\psi|\,\mathbf{P}_i\,|\psi\rangle$ and the state collapses to $\frac{\mathbf{P}_i|\psi\rangle}{\sqrt{\langle\psi|\mathbf{P}_i|\psi\rangle}}$.

$\mathbf{I}$ is the identity matrix (of appropriate dimension).

1. *Consider the partial measurement of the first qubit in an n qubit system. Express this partial measurement is as projective measurement.*
2. *The measurements discussed in class have the following (collapsing) property: once the measurement is applied to an n-qubit system, the state collapses to one of $\{|x\rangle\}_{x\in\{0,1\}^n}$, and any further measurements produce the same measurement. Does this property hold true for projective measurements?*

The most general class of measurements are Positive Operator Valued Measurements *(POVMs). These are defined using t Hermitian psd matrices $\mathcal{M} = \{\mathbf{M}_i\}_{i\in[t]}$ such that $\sum_i \mathbf{M}_i = \mathbf{I}$. When the POVM $\mathcal{M}$ is applied to pure state $|\psi\rangle$, the probability of measurement output being i is $\langle\psi|\,\mathbf{M}_i\,|\psi\rangle$. However, unlike prior notions of measurements where we also have a post-measurement quantum state, here we don't have such a state.*

In class, we showed that any mixed state is a pure state on a larger system. Similarly, any POVM is just a projective measurement on a larger system.

3. *Let $\mathcal{M} = \{\mathbf{M}_i\}_{i\in[t]}$ be a POVM applied to an n qubit pure state $|\psi\rangle$. Show that there exists a projective measurement $\mathcal{P} = \{\mathbf{P}_i\}_{i\in[t]}$ on a larger system over $n + \log t$ qubits, and a pure state $|\psi'\rangle$ on $n + \log t$ qubits such that $\langle\psi|\,\mathbf{M}_i\,|\psi\rangle = \langle\psi'|\,\mathbf{P}_i\,|\psi'\rangle$ for all $i \in [t]$.*

Please feel free to discuss with me in case you're not sure how to start the last part.

The last part should explain why we can't talk about the 'state' of the system after POVM measurement. There can be multiple such projective measurements, and each will result in a different post-measurement state.

[NC16] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information (10th Anniversary edition)*. Cambridge University Press, 2016.