CSE622 (IQC), Introduction to Quantum Computing | **Duration: 3 hours**
Winter 2024, IIIT-Delhi | ***Date: May 10, 2024***

EndSem (111111 points)

Relevant course outcomes:

CO1 Explain the foundation principles of quantum computing.

CO2 Use different quantum computing models for applications like search, numerical algorithms, cryptography, etc.

CO3 Design and/or analyse quantum algorithms and circuits.

Problem 1 (CO1,CO2). *(Points :6)* Suppose Alice and Bob share the entangled state $\frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle$.

(a) [2 points] Let U be any single-qubit operator. Suppose Alice applies U to her qubit. Show that the state of the entire system would be exactly same if instead of Alice, Bob had applied $U^\dagger$ to his qubit.
Hint: Any single qubit U can be expressed as $a|0\rangle\langle 0| + b|0\rangle\langle 1| - b^*|1\rangle\langle 0| + a^*|1\rangle\langle 1|$.

(b) [2 points] How would you describe the state of Bob after Alice has applied U to her qubit and then measured it in the standard basis (but did not communicate her measurement outcome to Bob)? Explain.

(c) [1 points] Would Bob's state after (b) be a mixed (non-pure) state? Explain.

(d) [1 point] Would Alice's state after (b) be a mixed (non-pure) state? Explain.

Problem 2 (CO1). *(Points :5)* These questions are about measurement operators.

(a) [1 point] If X is used as a projective measurement operator, then it refers to measurement in what basis?

(b) [1 point] Write down a POVM corresponding to the X projective measurement operator.

(c) [3 points] Now, consider these operators: $E_1 = |0\rangle\langle 0|$, $E_2 = |+\rangle\langle +|$, $E_3 = I - E_1 - E_2$. Does E_1, E_2, E_3 constitute a POVM ? Explain.

Problem 3 (CO2,CO3). *(Points :10)* Consider an n-qubit register initialized to some integer a; you may assume that $a \in \{0, \ldots, 2^n - 3\}$. Let b denote the integer $a + 2$. Let $|\psi\rangle = QFT_{2^n}|a\rangle$ and $|\psi'\rangle = QFT_{2^n}|b\rangle$.

For the quantum circuits below, you are allowed to use any single-qubit gates and their controlled versions.

(a) [1 point] Write the state $QFT_{2^n}|2^n - 2\rangle$ as a superposition over standard-basis states.

(b) [2 points] Draw a quantum circuit to map $|\psi'\rangle \to |b\rangle$. Explain, at a high level (3-4 sentences), what your circuit is doing.

(c) [5 points] Draw a quantum circuit to map $|\psi\rangle \to |\psi'\rangle$. Explain, at a high level (3-4 sentences), what your circuit is doing.

(d) [2 points] State the definition of $\|A\|_{op}$. Then, calculate the operator norm $\|QFT_{2^n}\|_{op}$?

Problem 4 (CO2,CO3). *(Points :18)* The subset-sum problem takes as input a set of integers $A = \{a_1, a_2, \dots a_n\}$ and a target integer T. Its goal is to decide whether A has a subset whose sum is exactly T. We can solve it using the following Boolean optimization problem in which n binary decision variables $x_1, \dots x_n$ are used; $x_i = 1$ indicates that a_i in included in the subset.

$$\min(T - \sum_{i=1}^{n} a_i x_i)^2$$

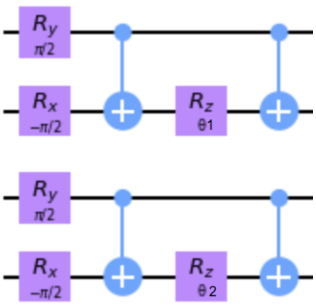
Parts (d) and (f) involve a lot of calculations. Use time judiciously.

(a) [3+1=4 points] Suppose we want to solve this problem using VQE. For the sake of concreteness, consider this instance: $A = \{1, 3, 4, 8\}$ and $T = 6$. Write down a suitable Ising Hamiltonian H representing the problem on this instance, and also write down the ground state energy of H.

(b) [3 points] Write down the Pauli-X,Y,Z matrices. *You need to know these correctly for the rest of the subparts. So, if you do not remember them correctly, you can get their answer from me; of course, you will not get marks for that matrix.*

(c) [3 points] Write down these operators $R_X(\alpha), R_Y(\alpha), R_Z(\alpha)$ in their matrix or outer-product forms. *Hint: You can use this definition* $R_P(\alpha) = e^{iP\frac{\alpha}{2}}$ *for any Pauli matrix* P.

(d) [4 points] Now, you have implemented a parameterized quantum circuit $C(\theta_1, \theta_2)$ given below to obtain an ansatz as required for VQE. Write down the ansatz $|\psi(\theta_1, \theta_2)\rangle$; you can use $|0000\rangle$ as the initial state.



(e) [1 point] State the variational principle and explain in 1-2 sentences how VQE can use that to compute the ground state energy of the Hamiltonian in (a).

(f) [3 points] For simplicity, consider a simpler Hamiltonian $H = \frac{5}{2}Z_1Z_2 - \frac{3}{4}Z_3$ (instead of the one you obtained in (a)). Calculate $\langle H \rangle$ (expectation value of H) for the state $|\psi(\frac{\pi}{2}, \frac{\pi}{2})\rangle$. Show your steps.

Problem 5 (CO2,CO3). *(Points :4)* In class we studied the quantum teleportation protocol in which Alice and Bob shared a Bell state. In this question, you will do the same but for the scenario when Alice and Bob share another Bell state $\frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle$.

(a) [2 points] Write down the state of Alice just before she performs the measurement step. Show your calculations.

(b) [2 points] Explain what operations Bob will perform for each message he receives from Alice.

Problem 6 (CO3). *(Points :10)* Let $f : \{0,1\}^n \to \{0,1\}$ be an n-bit to 1-bit function, and let U_f denote the corresponding phase oracle operator: $|x\rangle \to (-1)^{f(x)} |x\rangle$. Consider the following circuit: (1) Start with a register $|0^n\rangle$. (2) Apply $H^{\otimes n}$. (3) Apply U_f. (4) Apply $H^{\otimes n}$.

(a) [2 points] Derive the final state $|\psi\rangle$ after the above operations.

(b) [1 point] Derive the expression representing the probability $p(t)$ of observing $|t\rangle$ if $|\psi\rangle$ is measured in the standard basis.

(c) [3 points] Now, suppose it is known that there is some secret s such that $f(x) = f(x \oplus s)$ for all x. Now, take any t such that $s \cdot t$ is odd; prove that $p(t) = 0$.
This shows that if $|t\rangle$ is observed, i.e., $p(t) > 0$, then $s \cdot t = 0 (mod 2)$. So, if we find enough independent t, then we should be able to calculate s. However, the requirement may not always be satisfied.

(d) [2+2=4 points] Further, suppose there is another secret d such that $f(d) = f(d \oplus s) = 1$ and $f(x) = 0$ for all other values of x. Now, for this scenario, compute $p(0)$ and $p(t)$ for any $t \neq 0$.

Problem 7 (CO2,CO3). *(Points :10)* You are about to implement Grover's algorithm to search an unsorted N-sized array for any marked element. You happen to know that the fraction of marked elements is $p = \sin^2\theta$ (for some $\theta \in (0, \frac{\pi}{2})$). You have access to an oracle V that acts as:

$$V|i\rangle \to -|i\rangle \quad \text{if } A[i] \text{ is a marked element,}$$

$$V|i\rangle \to |i\rangle \quad \text{if } A[i] \text{ is not a marked element}$$

Grover's search algorithm is an application of the amplitude amplification algorithm that we studied in class. Amplitude amplification algorithms require two oracles: a state-preparation oracle (that we denoted A in our lectures), and a verification oracle for which you will use V.

(a)[1 point] How would you implement the state-preparation oracle A?

(b) [2 point] How would you implement the Grover iterator G? Mention the components of the operators, and for the components other than V and A, roughly describe how you would implement them.

(c) [1 point] Now, consider your implementation of Grover's algorithm to search the array for any marked element. Suppose $p \ll \frac{1}{10}$, and you want a low probability of error (say, at most $\frac{1}{10}$). How many calls to G would your implementation make? You should be able to compute this precisely since you know p. Explain how you arrived at your answer.

(d) [6 points] Suppose you know that $p \geq \frac{1}{4}$. Design an approach that requires only one call to G, and returns a marked solution with probability 1.
Hint: It will be difficult to control the angle of rotation induced by G, if you know what I mean. An easier approach would be to modify A so that one call to G suffices.

All the best!