CSE622 W20/Quantum Computing: Homework 5

Due date: 25th April 2024 (11:59pm)

Announced: 15th April 2024

1. [8 points] Let a be an n-bit integer. Consider the mapping: $F : \mathcal{H}^{2^n} \to \mathcal{H}^{2^n}$ specified as

$$F|a\rangle = |(a+1) \mod (2^n)\rangle.$$

(a)[1 point] Explain why F should be unitary.

(b)[3 point] Design a quantum circuit of $O(n)$-depth to map $QFT_{2^n}|a\rangle \to QFT_{2^n}|(a+1) \mod (2^n)\rangle$. You will get atmost 2 if you use 1 ancillæ(you need to perform clean computation); 2 or more ancilla cannot be used. Discuss the depth and size (number of gates) used in your implementation.

(c)[1 point] Use the idea of (b) to design a quantum circuit for the mapping F. Discuss the size and depth of your implementation.

(d)[3 points] Now, let b be another n-bit integer. Consider the unitary mapping $A|a\rangle|b\rangle = |a\rangle|(a+b) \mod (2^n)\rangle$. Design a quantum circuit for A, preferably without any ancillæ, but with at most 1. You should be able to use the idea in (c) and design a $O(poly(n))$-sized circuit. Discuss the depth and size of your implementation.

2. [4 points] Let $f : \{0,1\}^n \to \{0,1\}$ be an unknown Boolean function. You are given an oracle U_f for this function.

(a)[2 points] Suppose you are told that $f(x \oplus s) = f(x)$ for all x and some non-zero secret $s \in \{0,1\}^n$ (do you see that this is weaker than the promise in the Simon's problem?). Now, suppose you implemented the quantum circuit for the Simon's problem using U_f. Explain why the observation output (of the first register) is always some t such that $t \cdot c = 0$.

(b)[2 points] Observe that the observed t in (a) could be 0^n! Now, apart from the condition in (a), further suppose you are told that there is some d such that $f(d) = f(d \oplus s) = 1$ and $f(x)$ for all other values of x. What is the probability of observing a non-zero t for the quantum circuit in (a)?

You should now be able to design and analyse an algorithm like that of Simon's to identify the secret s with high probability. The calculations become a bit messy here, so this part is not included in the homework.

3. [4 points] The quantum circuit for QFT_{2^n} that we saw in class has complexity $O(n^2)$ and we also saw another optimized version with complexity $\omega(n \log n)$. Show that it is possible to design a quantum circuit C of complexity $O(n \log n)$ that approximates QFT_{2^n} in the sense that $\|C - QFT_{2^n}\| < \frac{1}{n}$.

4. [4 points] Imagine a quantum system of two parties, Alice (n_1 qubits) and Bob (n_2 qubits). Consider an arbitary state of the system in which the qubits are in an entangled state – the state was created when they were together. Now they are far apart, and suppose Bob wants to perform some operation on his qubits and then measure them using a projective measurement. But, Bob does not know if Alice has applied any unitary operation on her qubits in the meantime. Show the following:

[3 points] Let ρ_B^1 be the state of Bob's systems when they separated, let U_A be the unitary operator that Alice applied after separation, and let ρ_B^2 be the current state of Bob's system. Show that $\rho_B^1 = \rho_B^2$. This shows that Bob need not worry about any unitary operation that Alice may have applied.

[1 point] Does the above hold if Alice had performed a (projective) measurement $\{P_1, P_2, \ldots P_k\}$ instead of U_A? Of course, now that Alice and Bob do not want to talk to each other, Bob has no way of knowing what Alice observed and the post-measurement state of her system.

This justifies the step that we undertook to analyse Simon's algorithm in which we measured the second register just to simplify our analysis.

5.[5 points] In HW2, you implemented U_g for a balanced function g; consider its phase version $\hat{U}_g$. Further, consider the projector $P = |1\rangle\langle 1| \otimes |0\rangle\langle 0| \otimes I \otimes I$. Now, let $|\psi\rangle$ denote the state $\hat{U}_g H^{\otimes 4}|0000\rangle$, and suppose we represent it as $|\psi\rangle = \alpha_g|\psi_g\rangle + \alpha_b|\psi_b\rangle$ in which $|\psi_g\rangle = P|\psi\rangle/\|P|\psi\rangle\|$, $\alpha_g = \|P|\psi\rangle\|$; similarly, $|\psi_b\rangle$ denotes the normalized form of $(I-P)|\psi\rangle$, and α_b is the corresponding normalization factor.

In this homework, you will estimate $|\alpha_g|^2$ by implementing the amplitude estimation algorithm.

(a) [1 point] State $g()$ from HW2. Now, write down $|\psi_g\rangle$, $|\psi_b\rangle$, α_g, and α_b.

(b) [4 point] Now use the amplitude estimation algorithm to estimate $|\alpha_g|^2$ using QISKIT with probability of error 5%. Present a plot showing how the difference of the actual value and the estimate varies as the precision of estimation varies from 1 bit to 10 bits. You may use QISKIT libraries to implement your algorithm (i.e., you are NOT required to implement all the operations from scratch).