CS 410/510 Introduction to Quantum Computing

Homework 3

Portland State U, Spring 2017 — *May 2, 2017*
Lecturer: Fang Song — *Due: May 16, 2017*

Instructions. Your solutions will be graded on *correctness* and *clarity*. You should only submit work that you believe to be correct; if you cannot solve a problem completely, you will get significantly more partial credit if you clearly identify the gap(s) in your solution. It is good practice to start any long solution with an informal (but accurate) "proof summary" that describes the main idea. For this problem set, a random subset of problems will be graded. Problems marked with "**[G]**" are required for graduate students. Undergraduate students will get bonus points for solving them.

You may collaborate with others on this problem set. However, you must ***write up your own solutions*** and ***list your collaborators*** for each problem.

1. (Shor's algorithm) In this problem, we study further properties of quantum Fourier transform, and analyze Shor's algorithm for order finding that we've seen briefly in class. Recall the Quantum Fourier Transform $QFT_{\mathbb{Z}_M}$ for some integer M:

$$|\alpha\rangle = \sum_{x=0}^{M-1} \alpha_x |x\rangle \quad \overset{QFT_{\mathbb{Z}_N}}{\longmapsto} \quad |\hat{\alpha}\rangle = \sum_{y=0}^{M-1} \hat{\alpha}_y |y\rangle$$

where $\hat{\alpha}_y = \frac{1}{\sqrt{M}} \sum_x \omega_M^{xy}$, $\omega_N = e^{2\pi i/M}$, for each $y \in [M]$.

   (a) (5 points) Index shift. Let $j \in \mathbb{Z}_M$, and define $|\alpha_{+j}\rangle := \sum_x \alpha_x |x + j \bmod M\rangle$. Compute $|\hat{\alpha}_{+j}\rangle := QFT_{\mathbb{Z}_M}|\alpha_{+j}\rangle =$?. Justify from your result that measuring $|\hat{\alpha}\rangle$ and $|\hat{\alpha}_{+j}\rangle$ produce the same probability distribution.

   (b) (8 points) Periodic superposition. Consider an integer r such that $M = \ell \cdot r$ for some $\ell \in \mathbb{Z}$. Define $|P_r\rangle := \frac{1}{\sqrt{\ell}} \sum_{k=0}^{\ell-1} |kr\rangle = \frac{1}{\sqrt{\ell}}(|0\rangle + |r\rangle + \ldots + |(\ell-1)r\rangle)$. Show that applying $QFT_{\mathbb{Z}_M}$ on $|P_r\rangle$ gives $\frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} |k\ell\rangle = \frac{1}{\sqrt{r}}(|0\rangle + |\ell\rangle + \ldots + |(r-1)\ell\rangle)$.

   (c) (12 points) We can use the properties above to analyze Shor's order finding algorithm as illustrated in the circuit below. Our goal is to find the order of a mod a positive integer N, namely the smallest r such that $a^r = 1 \bmod N$. $E_a : |x\rangle|y\rangle \mapsto |x\rangle|y + a^x \bmod N\rangle$ is the unitary circuit implementing the modular exponentiation function $x \in \mathbb{Z}_{2^m} \mapsto a^x \bmod N$.

      i) What is the quantum state right after applying E_a? Since the bottom register will never be used, we may assume that it gets measured immediately. What do you see as the measurement outcome? Suppose that the outcome is z, what is the state on the top register then?

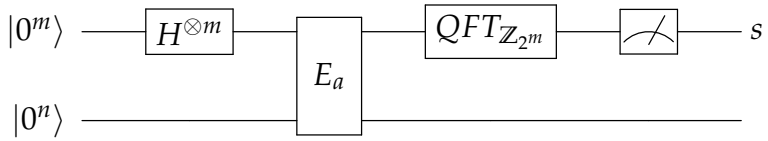

Figure 1: Shor's algorithm

ii) Then QFT is applied on top followed by a measurement, we call the outcome a sample s. Suppose that in this simple case, we are able to pick m such that $r|2^m$. Show how to use multiple samples to recover the order of a with high probability.

(d) (Exercise. You do not need to turn it in.) In general, we do not know an m such that $r|2^m$ to run Shor's algorithm. Describe how to compute the order $\mathrm{ORD}_N(a)$ then. Note: the core technique in Shor's algorithm is usually referred to as *Fourier sampling* as it produces random samples from the Fourier transform of the function. Conceptually, you may view order finding as a hidden subgroup problem on $\mathbb{Z}$ given the function $x \in \mathbb{Z} \mapsto a^x \bmod N$, and Shor's algorithm uses QFT_{2^m} in order to *approximately* Fourier sample over $\mathbb{Z}$.

2. (Grover's algorithm) This problem explores extensions of Grover's search algorithm. Consider as usual a function $f : \{0,1\}^n \to \{0,1\}$. Define $A = f^{-1}(1) := \{x \in \{0,1\}^n : f(x) = 1\}$ and $B = f^{-1}(0) := \{x \in \{0,1\}^n : f(x) = 0\}$. Let $a = |A|$ be the number of "marked" items and $b = N - a$ where $N = 2^n$. We further define $|A\rangle := \frac{1}{\sqrt{a}} \sum_{x \in A} |x\rangle$ and $|B\rangle := \frac{1}{\sqrt{b}} \sum_{x \in B} |x\rangle$.

(a) (5 points) Run Grover's algorithm with f on input $|0^n\rangle$. Namely we apply unitary $G := -HZ_0HZ_f$ repetitively on $H|0^n\rangle$ where $Z_0 : |x\rangle \mapsto -|x\rangle$ iff. $x = 0^n$ and $Z_f : |x\rangle \mapsto (-1)^{f(x)}|x\rangle$. Denote $|\psi^0\rangle = H|0^n\rangle$ and $|\psi^t\rangle := G^t|\psi^0\rangle$ for $t \geq 1$. Show that every $|\psi^t\rangle$ can be written as $\cos(\theta_t)|A\rangle + \sin(\theta_t)|B\rangle$. How does θ_t change to θ_{t+1}? (Hint: geometric interpretation of Grover's algorithm)

(b) (5 points) Show that if we pick t to be the nearest integer to $\frac{1}{2}(\frac{\pi}{2\theta_0} - 1)$, $|\langle\psi^t|A\rangle|^2 \geq 1/2$. This implies that measuring $|\psi^t\rangle$ will output an element x of A with probability at least $1/2$. What is the distribution of x, conditioned on being in A?

(c) (5 points) Assuming a is known to us. How to find an element of A with high probability using $O(\sqrt{N/a})$ queries to the oracle?

(d) (7 points) What if a is unknown? Show that if one picks $t \in \{1, \ldots, \sqrt{N} + 1\}$ at random and run Grover's algorithm, it succeeds in finding a marked element with probability at least $1/4$.

(e) (10 points) Show how to find a marked item with high probability within $O(\sqrt{N/a})$ queries. (Hint: pick random $t \in \{1, \ldots T\}$ with a small T in the beginning and try. If fail increment T slowly but exponentially.)

(f) (10 points) **[G]** One natural application of Grover's algorithm is finding the minimum element in a list of N numbers. Give a $O(\sqrt{N})$ quantum algorithm. (Hint: can you pick a *random* pivot element every time that is smaller than the current pivot element? Part b) may be helpful.)

3. (Mixed states and density matrix)

   (a) (5 points) A density matrix corresponds to a pure state if and only if $\rho = |\psi\rangle\langle\psi|$. Show that ρ corresponds to a pure state if and only if $Tr(\rho^2) = 1$.

   (b) (5 points) Show that every 2×2 density matrix ρ can be expressed as an equally weighted mixture of pure states. That is $\rho = \frac{1}{2}|\psi_1\rangle\langle\psi_1| + \frac{1}{2}|\psi_2\rangle\langle\psi_2|$ (Note: the two states do not need to be orthogonal).

   (c) (5 points) Imagine two parties Alice and Bob. Alice flips a biased coin which is HEADS with probability $\cos^2(\pi/8)$. Alice prepares $|0\rangle$ when she sees coin 0 and $|1\rangle$ otherwise. From Alices perspective (who knows the coin value), the density matrix of the state she created will be either $|0\rangle\langle 0|$ or $|1\rangle\langle 1|$. She then sends the qubit to Bob. What is the density matrix of the state from Bobs perspective (who does not know the coin value)? Write down the matrix.

4. (8 points) (Teleporting part of an entangled state.) Recall that, in the teleportation protocol, Alice and Bob initially have a joint state of the form $(\alpha|0\rangle_A + \beta|1\rangle_A)\frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB})$. (Subscripts indicate who possesses each qubit). At the end of the protocol, there remains only Bobs qubit, and it is in state $\alpha|0\rangle_B + \beta|1\rangle_B$. Now we introduce a third party, Carol. Suppose that Alice possesses a qubit that she want to teleport to Bob, and this qubit is entangled with Carols qubit, in state $\frac{1}{\sqrt{2}}|00\rangle_{CA} + |11\rangle_{CA}$. Set the initial state to

$$\frac{1}{\sqrt{2}}(|00\rangle_{CA} + |11\rangle_{CA}) \otimes \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB}) .$$

   Perform the teleportation protocol on Alices and Bobs qubits. At the end of the protocol, there will remain two qubits: Carols and Bobs. What is the state of Carol and Bobs qubits? Justify your answer by a clear proof.